

Produkthandbuch

McAfee Enterprise Security Manager 9.5.0

COPYRIGHT

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

MARKEN

Intel und das Intel-Logo sind eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. McAfee und das McAfee-Logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource und VirusScan sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.

LIZENZINFORMATIONEN

LIZENZVEREINBARUNG

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWARE-PAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSEITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN McAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einleitung **9**

Informationen zu diesem Handbuch 9

Zielgruppe 9

Konventionen 9

Quellen für Produktinformationen 10

1 Einleitung **11**

Funktionsweise von McAfee Enterprise Security Manager 11

Geräte und ihre Funktion 12

2 Erste Schritte **13**

Informationen zum FIPS-Modus 13

Informationen zum FIPS-Modus 14

Auswählen des FIPS-Modus 14

Überprüfen der FIPS-Integrität 15

Hinzufügen eines Geräts mit festgelegtem Schlüssel im FIPS-Modus 16

Fehlerbehebung für den FIPS-Modus 20

Zertifizierte Common Criteria-Konfiguration 20

An- und Abmelden 21

Anpassen der Anmeldeseite 22

Aktualisieren der ESM-Software 23

Anfordern und Hinzufügen von Anmeldeinformationen für Regelaktualisierungen 23

Überprüfen auf Regelaktualisierungen 24

Ändern der Sprache für Ereignisprotokolle 25

Verbinden von Geräten 25

Hinzufügen von Geräten zur ESM-Konsole 25

Auswählen eines Anzeigetyps 26

Verwalten benutzerdefinierter Anzeigetypen 26

Verwalten einer Gruppe in einem benutzerdefinierten Anzeigetyp 27

Löschen einer Gruppe oder eines Geräts 28

Löschen doppelter Geräte in der Systemnavigationsstruktur 28

Konsoleneinstellungen 29

ESM-Konsole 29

Arbeiten mit dem Farbdesign für die Konsole 30

Auswählen von Einstellungen für die Konsolenansicht 30

Festlegen des Zeitüberschreitungswerts für die Konsole 30

Auswählen von Benutzereinstellungen 30

Einrichten von Benutzeranmeldeinformationen für McAfee ePO 31

3 Konfigurieren von ESM **33**

Verwalten von Geräten 33

Anzeigen der Gerätestatistik 35

Hinzufügen von Geräten zur ESM-Konsole 36

Informationen zu Geräteschlüsseln 37

Aktualisieren der Software eines Geräts 39

Anordnen der Geräte . . . 39
Verwalten mehrerer Geräte . . . 56
Verwalten von URL-Links für alle Geräte . . . 56
Anzeigen von Zusammenfassungsberichten für Geräte . . . 56
Anzeigen eines System- oder Geräteprotokolls . . . 57
Berichte zum Integritätsstatus von Geräten . . . 57
Löschen einer Gruppe oder eines Geräts . . . 60
Aktualisieren der Geräte . . . 60
Konfigurieren von Geräten . . . 61
Geräte und ihre Funktion . . . 62
Event Receiver-Einstellungen . . . 63
Einstellungen für Enterprise Log Manager (ELM) . . . 120
Einstellungen für Advanced Correlation Engine (ACE) . . . 136
Einstellungen für Application Data Monitor (ADM) . . . 140
Einstellungen für Database Event Monitor (DEM) . . . 155
Einstellungen für verteilte ESM-Geräte (DESM) . . . 163
ePolicy Orchestrator-Einstellungen . . . 164
Einstellungen für Nitro Intrusion Prevention System (Nitro IPS) . . . 170
McAfee Vulnerability Manager-Einstellungen . . . 174
McAfee Network Security Manager-Einstellungen . . . 176
Konfigurieren von zusätzlichen Diensten . . . 177
Allgemeine Systeminformationen . . . 177
Konfigurieren von Remedy-Server-Einstellungen . . . 178
Definieren von Nachrichteneinstellungen . . . 178
Einrichten von NTP auf einem Gerät . . . 179
Konfigurieren von Netzwerkeinstellungen . . . 180
Systemzeitsynchronisierung . . . 186
Installieren eines neuen Zertifikats . . . 187
Konfigurieren von Profilen . . . 188
SNMP-Konfiguration . . . 188
Verwalten der Datenbank . . . 195
Einrichten des ESM-Datenspeichers . . . 196
Einrichten des ESM-VM-Datenspeichers . . . 196
Erhöhen der Anzahl verfügbarer Akkumulator-Indizes . . . 196
Einrichten des Archivs für inaktive Partitionen . . . 197
Einrichten von Datenbeibehaltungs-Limits . . . 197
Definieren von Datenzuordnungslimits . . . 198
Verwalten von Indexeinstellungen für die Datenbank . . . 198
Verwalten der Akkumulator-Indizierung . . . 198
Anzeigen der Speicherverwendung der Datenbank . . . 199
Arbeiten mit Benutzern und Gruppen . . . 199
Hinzufügen eines Benutzers . . . 200
Auswählen von Benutzereinstellungen . . . 200
Einrichten der Sicherheit . . . 201
Einrichten von Benutzeranmeldeinformationen für McAfee ePO . . . 204
Deaktivieren oder erneutes Aktivieren eines Benutzers . . . 205
Authentifizieren von Benutzer gegenüber einem LDAP-Server . . . 205
Einrichten von Benutzergruppen . . . 206
Hinzufügen einer Gruppe mit eingeschränktem Zugriff . . . 206
Sichern und Wiederherstellen von Systemeinstellungen . . . 206
Sichern von ESM-Einstellungen und Systemdaten . . . 207
Wiederherstellen der ESM-Einstellungen . . . 207
Wiederherstellen gesicherter Konfigurationsdateien . . . 208
Arbeiten mit Sicherungsdateien in ESM . . . 208
Verwalten der Dateiwartung . . . 209
Redundantes ESM-Gerät . . . 209

Verwalten des ESM-Geräts . . . 211
Verwalten von Protokollen . . . 212
Maskieren von IP-Adressen . . . 213
Einrichten der ESM-Protokollierung . . . 214
Ändern der Sprache für Ereignisprotokolle . . . 214
Exportieren und Wiederherstellen von Kommunikationsschlüsseln . . . 214
Erneutes Generieren des SSH-Schlüssels . . . 215
Task-Manager für Abfragen . . . 215
Verwalten von Abfragen, die in ESM ausgeführt werden . . . 216
Aktualisieren eines primären oder redundanten ESM-Geräts . . . 216
Zugreifen auf ein Remote-Gerät . . . 217
Verwenden von Linux-Befehlen . . . 217
Verfügbare Linux-Befehle . . . 218
Verwenden einer globalen Blacklist . . . 218
Einrichten einer globalen Blacklist . . . 219
Was ist Datenanreicherung? . . . 220
Hinzufügen von Datenanreicherungsquellen . . . 220
Einrichten der Datenanreicherung durch McAfee Real Time for McAfee ePO™ . . . 220
Hinzufügen einer Hadoop HBase-Datenanreicherungsquelle . . . 221
Hinzufügen einer Hadoop Pig-Datenanreicherungsquelle . . . 222
Hinzufügen von Active Directory-Datenanreicherung für Benutzernamen . . . 222

4 Verwalten von Cyber-Bedrohungen 225
Einrichten der Cyber Threat-Verwaltung . . . 225
Anzeigen von Ergebnissen eines Cyber Threat-Feeds . . . 226

5 Arbeiten mit Inhaltspaketen 229
Importieren von Inhaltspaketen . . . 229

6 Arbeiten mit Alarmen 231
Funktionsweise der ESM-Alarme . . . 231
Erstellen eines Alarms . . . 232
UCAPL-Alarme . . . 233
Einrichten eines Korrelationsalarms, der Quellereignisse enthalten soll . . . 235
Hinzufügen eines Alarms vom Typ Feldübereinstimmung . . . 236
Hinzufügen eines Alarms zu Regeln . . . 237
Erstellen eines SNMP-Traps als Aktion in einem Alarm . . . 237
Hinzufügen eines Alarms zur Benachrichtigung bei Stromausfällen . . . 238
Hinzufügen eines Alarms für Integritätsüberwachungsereignisse . . . 239
Kopieren eines Alarms . . . 247
Aktivieren oder Deaktivieren der Alarmüberwachung . . . 247
Anpassen der Übersicht für ausgelöste Alarme und Fälle . . . 248
Verwalten von Nachrichtenvorlagen für Alarme . . . 248
Verwalten von Audiodateien für Alarme . . . 249
Verwalten von Alarmempfängern . . . 249
Verwalten von Alarmen . . . 249
Anzeigen der Warteschlange für Alarmberichte . . . 250
Verwalten von Alarmberichtsdateien . . . 251

7 Arbeiten mit Ereignissen 253
Ereignisse, Flüsse und Protokolle . . . 253
Einrichten von Downloads für Ereignisse, Flüsse und Protokolle . . . 254
Begrenzen der Erfassungszeit für Daten . . . 254
Definieren der Einstellungen für den Schwellenwert für Inaktivität . . . 255
Abrufen von Ereignissen und Flüssen . . . 255
Überprüfen auf Ereignisse, Flüsse und Protokolle . . . 255

Definieren von Geolocation- und ASN-Einstellungen . . . 256
Abrufen von Ereignissen und Flüssen . . . 256
Aggregieren von Ereignissen oder Flüssen . . . 256
Einrichten der Ereignisweiterleitung . . . 259
Verwalten von Berichten . . . 263
Festlegen des Startmonats für Quartalsberichte . . . 264
Hinzufügen eines Berichts . . . 264
Hinzufügen eines Berichtslayouts . . . 265
Einschließen eines Bilds in PDF-Dateien und Berichte . . . 265
Hinzufügen einer Berichtsbedingung . . . 265
Anzeigen von Host-Namen in einem Bericht . . . 266
Beschreibung der *contains*-Filter und Filter für *reguläre Ausdrücke* . . . 266
Arbeiten mit ESM-Ansichten . . . 270
Verwenden von ESM-Ansichten . . . 270
Anzeigen von Sitzungsdetails . . . 271
Ansichtssymbolleiste . . . 271
Vordefinierte Ansichten . . . 272
Hinzufügen einer benutzerdefinierten Ansicht . . . 277
Ansichtskomponenten . . . 278
Arbeiten mit dem Abfragen-Assistenten . . . 290
Ansichten verwalten . . . 294
Untersuchen der umliegenden Ereignisse eines Ereignisses . . . 294
Anzeigen der Details zur IP-Adresse eines Ereignisses . . . 295
Ändern der Standardansicht . . . 295
Filtern von Ansichten . . . 296
Überwachungslisten . . . 299
Zeichenfolgennormalisierung . . . 302
Benutzerdefinierte Typfilter . . . 303
Erstellen benutzerdefinierter Typen . . . 305
Tabelle der vordefinierten benutzerdefinierten Typen . . . 305
Hinzufügen benutzerdefinierter Typen für die Uhrzeit . . . 309
Benutzerdefinierte Typen für Name/Wert . . . 309
Hinzufügen eines benutzerdefinierten Typs für eine Name/Wert-Gruppe . . . 309

8 Verwalten von Fällen 311
Hinzufügen eines Falls . . . 311
Erstellen eines Falls aus einem Ereignis . . . 312
Hinzufügen von Ereignissen zu einem vorhandenen Fall . . . 312
Bearbeiten oder Schließen eines Falls . . . 312
Anzeigen von Falldetails . . . 313
Hinzufügen von Fallstatusebenen . . . 313
Senden von Fällen per E-Mail . . . 314
Anzeigen aller Fälle . . . 314
Generieren von Fallverwaltungsberichten . . . 315

9 Arbeiten mit Asset Manager 317
Verwalten von Ressourcen . . . 318
Definieren alter Ressourcen . . . 318
Einrichten der Konfigurationsverwaltung . . . 318
Verwalten abgerufener Konfigurationsdateien . . . 319
Netzwerkerkennung . . . 319
Entdecken des Netzwerks . . . 319
Verwalten der IP-Ausschlussliste . . . 320
Entdecken von Endpunkten . . . 320
Anzeigen einer Netzwerkübersicht . . . 321
Ändern des Verhaltens der Netzwerkerkennung . . . 321

Ressourcenquellen . . . 321
Verwalten von Ressourcenquellen . . . 322
Verwalten von Vulnerability Assessment-Quellen . . . 322
Zonenverwaltung . . . 322
Verwalten von Zonen . . . 322
Hinzufügen einer Zone . . . 323
Exportieren von Zoneneinstellungen . . . 323
Importieren von Zoneneinstellungen . . . 323
Hinzufügen einer Teilzone . . . 324
Bewertung von Ressourcen, Bedrohungen und Risiken . . . 325
Verwalten bekannter Bedrohungen . . . 326

10 Verwalten von Richtlinien und Regeln 327
Grundlegendes zum Richtlinien-Editor . . . 327
Richtlinienstruktur . . . 328
Verwalten von Richtlinien in der Richtlinienstruktur . . . 329
Regeltypen und ihre Eigenschaften . . . 331
Variablen . . . 332
Präprozessorregeln . . . 335
Firewall-Regeln . . . 336
Deep Packet Inspection-Regeln . . . 338
Interne Regeln . . . 339
Filterregeln . . . 340
ASP-Regeln . . . 340
Datenquellenregeln . . . 342
Windows-Ereignisregeln . . . 343
ADM-Regeln . . . 344
DEM-Regeln . . . 345
Korrelationsregeln . . . 352
Anzeigen von Details zu Korrelationsregeln . . . 353
Hinzufügen benutzerdefinierter ADM-Regeln, Datenbankregeln oder Korrelationsregeln . . . 353
ESM-Regeln . . . 360
Normalisierung . . . 360
Aktivieren von Paket kopieren . . . 361
Einstellungen für Standardrichtlinien . . . 361
Reiner Warnungsmodus . . . 361
Einrichten des Überbelegungsmodus . . . 362
Anzeigen des Richtlinienaktualisierungsstatus für Geräte . . . 362
Regelvorgänge . . . 363
Verwalten von Regeln . . . 363
Importieren von Regeln . . . 364
Importieren von Variablen . . . 365
Exportieren von Regeln . . . 365
Festlegen der automatischen Aufnahme in die Blacklist durch Regeln . . . 366
Filtern vorhandener Regeln . . . 367
Anzeigen der Signatur einer Regel . . . 368
Abrufen von Regelaktualisierungen . . . 369
Löschen des aktualisierten Regelstatus . . . 369
Vergleichen von Regeldateien . . . 370
Anzeigen des Verlaufs der Regeländerungen . . . 370
Erstellen einer neuen Überwachungsliste mit Regeln . . . 370
Hinzufügen von Regeln zu einer Überwachungsliste . . . 371
Zuweisen von Tags zu Regeln oder Ressourcen . . . 372
Aggregationseinstellungen ändern . . . 373
Überschreibungsaktion für heruntergeladene Regeln . . . 373
Gewichtungen der Schweregrade . . . 374

Festlegen der Gewichtungen der Schweregrade 374
Anzeigen des Verlaufs der Richtlinienänderungen 375
Anwenden von Richtlinienänderungen 375
Verwalten von Datenverkehr mit Priorität 375

Index **377**

Einleitung

In diesem Handbuch finden Sie die erforderlichen Informationen für die Arbeit mit Ihrem McAfee-Produkt.

Inhalt

- *Informationen zu diesem Handbuch*
- *Quellen für Produktinformationen*

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation wurde von McAfee nach eingehender Recherche mit Blick auf die Zielgruppe verfasst.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren**: Personen, die für die Implementierung und Durchsetzung des Sicherheitsprogramms eines Unternehmens verantwortlich sind.
- **Benutzer**: Personen, die den Computer nutzen, auf dem die Software ausgeführt wird, und die auf einige oder alle Funktionen zugreifen können.

Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.
Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	**Hinweis:** Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	**Tipp:** Vorschläge und Empfehlungen.



Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.



Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Quellen für Produktinformationen

Nach der Veröffentlichung eines Produkts werden Informationen zu dem Produkt im Online-Knowledge Center von McAfee eingegeben.

Vorgehensweise

1 Rufen Sie im McAfee ServicePortal unter http://support.mcafee.com die Registerkarte **Knowledge Center** auf.

2 Klicken Sie im Bereich **Knowledge Base** auf eine Inhaltsquelle:

- **Produktdokumentation** für die Suche nach Benutzerdokumentation
- **Technische Artikel** für die Suche nach KnowledgeBase-Artikeln

3 Wählen Sie **Meine Filter nicht löschen** aus.

4 Geben Sie ein Produkt ein, und wählen Sie die Version aus. Klicken Sie dann auf **Suchen**, um eine Liste der gewünschten Dokumente anzuzeigen.

1 Einleitung

Experten für Sicherheit und Compliance können mit McAfee® Enterprise Security Manager (McAfee ESM) Risiken und Bedrohungen zentral erfassen, speichern, analysieren und entsprechende Maßnahmen ergreifen.

Inhalt

- *Funktionsweise von McAfee Enterprise Security Manager*
- *Geräte und ihre Funktion*

Funktionsweise von McAfee Enterprise Security Manager

Mit McAfee ESM werden Daten und Ereignisse aus Sicherheitsgeräten, Netzwerkinfrastrukturen, Systemen und Anwendungen erfasst und aggregiert. Diese Daten werden dann mit weiteren Informationen kombiniert, das heißt mit Kontextinformationen zu Benutzern, Ressourcen, Schwachstellen und Bedrohungen. Diese Informationen werden korreliert, um relevante Vorfälle zu finden. Mithilfe interaktiver anpassbarer Dashboards können Sie bestimmte Ereignisse weiter aufgliedern, um Vorfälle zu untersuchen.

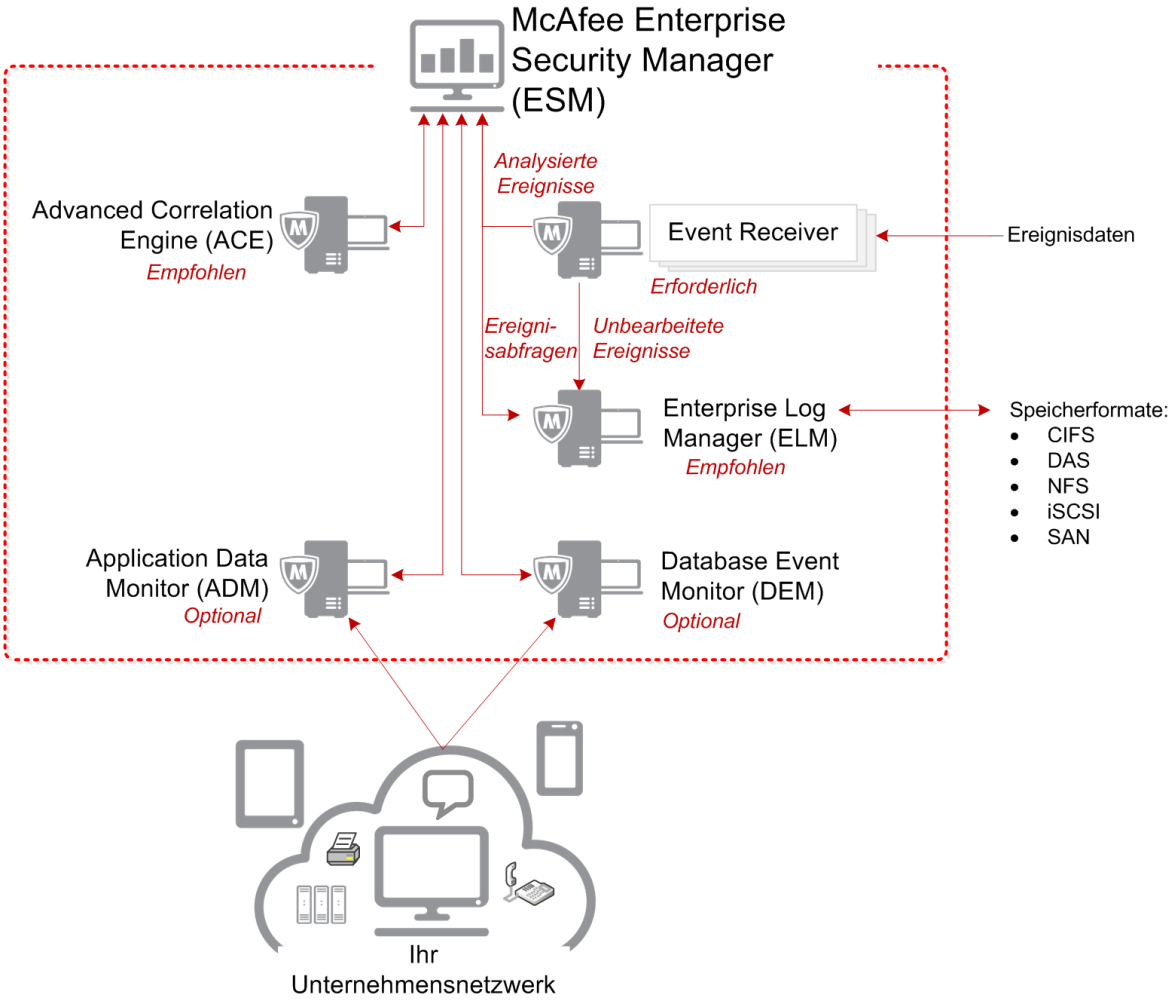
ESM besteht aus drei Schichten:

- **Benutzeroberfläche**: Ein Browser-Programm, das die Schnittstelle zwischen Benutzer und System darstellt und als *ESM-Konsole* bezeichnet wird.
- **Datenspeicher, -verwaltung und -analyse**: Diese Geräte stellen alle notwendigen Dienste für die Datenbearbeitung wie beispielsweise Konfiguration, Berichterstellung, Visualisierung und Suche bereit. Für diese Funktionen verwenden Sie ESM (erforderlich), Advanced Correlation Engine (ACE), Distributed ESM (DESM) und Enterprise Log Manager (ELM).
- **Datenerfassung**: Diese Geräte stellen die Schnittstellen und Dienste bereit, über die Daten aus der Netzwerkumgebung der Benutzer erfassen werden. Für diese Funktionen verwenden Sie Nitro Intrusion Prevention System (IPS), Event Receiver (Empfänger), Application Data Monitor (ADM) und Database Event Monitor (DEM).

Alle Befehls-, Steuerungs- und Kommunikationsfunktionen zwischen den Komponenten werden über sichere Kommunikationskanäle koordiniert.

Geräte und ihre Funktion

Mit dem ESM-Gerät können Sie alle physischen und virtuellen Geräte in einer Sicherheitsumgebung verwalten und mit den Geräten interagieren.



Siehe auch

Event Receiver-Einstellungen auf Seite 63
Einstellungen für Enterprise Log Manager (ELM) auf Seite 120
Einstellungen für Application Data Monitor (ADM) auf Seite 140
Einstellungen für Database Event Monitor (DEM) auf Seite 155
Einstellungen für Advanced Correlation Engine (ACE) auf Seite 136
Einstellungen für verteilte ESM-Geräte (DESM) auf Seite 163
ePolicy Orchestrator-Einstellungen auf Seite 164
Einstellungen für Nitro Intrusion Prevention System (Nitro IPS) auf Seite 170

2 Erste Schritte

Vergewissern Sie sich, dass die ESM-Umgebung auf dem aktuellen Stand und einsatzbereit ist.

Inhalt

- *Informationen zum FIPS-Modus*
- *Zertifizierte Common Criteria-Konfiguration*
- *An- und Abmelden*
- *Anpassen der Anmeldeseite*
- *Aktualisieren der ESM-Software*
- *Anfordern und Hinzufügen von Anmeldeinformationen für Regelaktualisierungen*
- *Überprüfen auf Regelaktualisierungen*
- *Ändern der Sprache für Ereignisprotokolle*
- *Verbinden von Geräten*
- *Konsoleneinstellungen*

Informationen zum FIPS-Modus

Der Federal Information Processing Standard (FIPS) umfasst öffentlich bekannt gegebene Standards der USA. Wenn Sie an diese Standards gebunden sind, müssen Sie das System im FIPS-Modus betreiben.



Sie müssen den FIPS-Modus bei der ersten Anmeldung beim System auswählen und können ihn später nicht mehr ändern.

Siehe auch

Informationen zum FIPS-Modus auf Seite 14

Inhalt

- *Informationen zum FIPS-Modus*
- *Auswählen des FIPS-Modus*
- *Überprüfen der FIPS-Integrität*
- *Hinzufügen eines Geräts mit festgelegtem Schlüssel im FIPS-Modus*
- *Fehlerbehebung für den FIPS-Modus*

Informationen zum FIPS-Modus

Aufgrund von FIPS-Vorschriften sind einige ESM-Funktionen nicht verfügbar, einige sind nicht konform, und einige sind nur im FIPS-Modus verfügbar. Diese hier aufgeführten Funktionen sind überall im Dokument mit Hinweisen versehen.

Status der Funktion	Beschreibung
Entfernte Funktionen	• Empfänger mit Hochverfügbarkeit • GUI-Terminal • Möglichkeit zum Kommunizieren mit dem Gerät über das SSH-Protokoll • In der Gerätekonsole wird die Root-Shell durch ein Menü für die Geräteverwaltung ersetzt.
Funktionen, die nur im FIPS-Modus verfügbar sind	• Es gibt vier Benutzerrollen ohne Überschneidung: **Benutzer**, **Power-User**, **Audit-Administrator** und **Administrator für Schlüssel und Zertifikate**. • Alle Seiten mit dem Titel **Eigenschaften** enthalten die Option **Selbsttest**, mit der Sie sich vergewissern können, dass das System erfolgreich im FIPS-Modus betrieben wird. • Bei Auftreten eines FIPS-Fehlers wird als Hinweis in der Systemnavigationsstruktur eine Statuskennzeichnung hinzugefügt. • Alle Seiten mit dem Titel **Eigenschaften** enthalten die Option **Ansicht**. Wenn Sie auf diese Option klicken, wird die Seite **FIPS-Identitäts-Token** geöffnet. Auf dieser Seite wird ein Wert angezeigt, den Sie mit dem Wert in den entsprechenden Abschnitten des Dokuments vergleichen müssen, um sicherzustellen, dass FIPS nicht kompromittiert wurde. • Wenn Sie auf die Optionen **Systemeigenschaften** | **Benutzer und Gruppen** | **Berechtigungen** | **Gruppe bearbeiten**klicken, enthält die Seite die Berechtigung **Selbsttest der FIPS-Verschlüsselung**. Damit werden die Gruppenmitglieder autorisiert, FIPS-Selbsttests auszuführen. • Wenn Sie auf **Schlüssel importieren** oder **Schlüssel exportieren** klicken (unter **IPS-Eigenschaften** | **Schlüsselverwaltung**), werden Sie aufgefordert, den Typ des zu importierenden oder exportierenden Schlüssels auszuwählen. • In **Assistent zum Hinzufügen von Geräten** ist das TCP-Protokoll immer auf Port 22 festgelegt. Der SSH-Port kann geändert werden.

Auswählen des FIPS-Modus

Bei der ersten Anmeldung beim System werden Sie aufgefordert, auszuwählen, ob Sie das System im FIPS-Modus betreiben möchten. Diese Auswahl kann später nicht geändert werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Gehen Sie bei der ersten Anmeldung bei ESM wie folgt vor:

   a Geben Sie in das Feld **Benutzername** die Zeichenfolge `NGCP` ein.

   b Geben Sie in das Feld **Kennwort** die Zeichenfolge `security.4u` ein.

   Sie werden aufgefordert, das Kennwort zu ändern.

2 Geben Sie das neue Kennwort ein, und bestätigen Sie es.

3 Klicken Sie auf der Seite **FIPS aktivieren** auf **Ja**.

In der Warnung zu **FIPS aktivieren** werden Sie aufgefordert, zu bestätigen, dass Sie das System dauerhaft im FIPS-Modus betreiben möchten.

4 Klicken Sie auf **Ja**, um die Auswahl zu bestätigen.

Überprüfen der FIPS-Integrität

Wenn Sie im FIPS-Modus arbeiten, muss die Integrität der Software gemäß FIPS 140-2 regelmäßig getestet werden. Diese Tests müssen Sie auf dem System und auf jedem einzelnen Gerät ausführen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und vergewissern Sie sich, dass **Systeminformationen** ausgewählt ist.

2 Führen Sie eine oder mehrere der folgenden Aktionen aus.

Feld	Vorgehensweise
FIPS-Status	Zeigen Sie die Ergebnisse des letzten auf dem ESM-Gerät ausgeführten FIPS-Selbsttests an.
Test oder **FIPS-Selbsttest**	Führen Sie die FIPS-Selbsttests aus. Dabei wird die Integrität der Algorithmen getestet, die in der ausführbaren Datei für die Kryptografie verwendet werden. Die Ergebnisse können Sie im **Nachrichtenprotokoll** anzeigen. Wenn der FIPS-Selbsttest fehlschlägt, ist FIPS kompromittiert, oder es liegt ein Gerätefehler vor. Wenden Sie sich an den McAfee-Support.
Ansicht oder **FIPS-Identitäts-Token**	Öffnen Sie die Seite **FIPS-Identitäts-Token**, um die Integrität der Software beim Einschalten zu testen. Vergleichen Sie den folgenden Wert mit dem auf dieser Seite angezeigten öffentlichen Schlüssel: -----BEGIN PUBLIC KEY----- MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAt8FWOP2mvVjvTTxkhGqk LdgA+sx0jBv+zYnCkGYOHHzNAdum9yuMn69GNbYXm7I5OcKv2+nz6axBruCZ5XX1 jCGWrmsj8YZJoNp/FLUy1jYE7lXI5/NRm2uhjhzjdOjgFv10SkgxVfL/aBJjqZFJ KKbHMzYEBwdyseQUc56u3mKaBtP4rydfRmEtytkuOsZgQuPHKYhaQJlnbV5LfrLa o6HQSlzHYHlcF/Yog+QHJ6ClSRA1lk8MPyFG9RHdKnwcq3sY8QjQMbIZ5SDobbK0 GPOOucG8vWDWdxSiabJLBdklVsmB0zwdH6lOCkkGTidayMk12hDh+2BA6el7YQBV 8EJaJ5wvz8aQKwDfiirnlb9vmC+sk+Rwo/E7uRn3El4+RxouHi9J3f92I9qXZeJCV iYV2XahhyxSpq8ro/j0BMTiab3dIjjogxMxCI9QjEpm3J/ZyUpWtNKaHq8BgSE1e daiJob7O/kvef1T/ZOb3O90bSK3vtn+3Si3K3cpaY/qBm9var6xVNyGhHztRJv0F 0nSJlyddWuXL1U+hMTO2YE33T3s4Uf4jiomTVSDTJ087hLT5l/hCz6A33Hzl7gk8 Q89SNsmL/p0RAJzJ3+mGyoUAd1D2u6sYq6NkGCn640a5A2zAOQdX/M8R8S+NKjgi nLg3n+/+25KsCB3KDY3AkYECAwEAAQ== -----END PUBLIC KEY----- Wenn dieser Wert und der öffentliche Schlüssel nicht übereinstimmen, ist FIPS kompromittiert. Wenden Sie sich an den McAfee-Support.

Hinzufügen eines Geräts mit festgelegtem Schlüssel im FIPS-Modus

Es gibt im FIPS-Modus zwei Methoden zum Hinzufügen eines Geräts, das bereits mit einem Schlüssel an ein ESM-Gerät gebunden wurde. Die folgenden Begriffe und Dateierweiterungen sind hilfreich, wenn Sie diese Verfahren anwenden.

Terminologie

- **Geräteschlüssel**: Enthält die Verwaltungsrechte, über die ein ESM-Gerät in Bezug auf ein Gerät verfügt, und wird nicht zu Kryptografiezwecken verwendet.
- **Öffentlicher Schlüssel**: Der öffentliche SSH-Kommunikationsschlüssel des ESM-Geräts, der in der Tabelle der autorisierten Schlüssel für ein Gerät gespeichert ist.
- **Privater Schlüssel**: Der private SSH-Kommunikationsschlüssel des ESM-Geräts, der von der ausführbaren SSH-Datei auf einem ESM-Gerät zum Herstellen der SSH-Verbindung mit einem Gerät verwendet wird.
- **Primäres ESM-Gerät**: Das ESM-Gerät, das ursprünglich zum Registrieren des Geräts verwendet wurde.
- **Sekundäres ESM-Gerät**: Das zusätzliche ESM-Gerät, das mit dem Gerät kommuniziert.

Dateierweiterungen für die verschiedenen Exportdateien

- **.exk**: Enthält den Geräteschlüssel.
- **.puk**: Enthält den öffentlichen Schlüssel.
- **.prk**: Enthält den privaten Schlüssel und den Geräteschlüssel.

Sichern und Wiederherstellen von Informationen für ein Gerät im FIPS-Modus

Mit dieser Methode können Sie Kommunikationsinformationen für ein Gerät in ESM sichern und wiederherstellen.

Diese Methode ist in erster Linie für die Verwendung im Fall eines Fehlers gedacht, aufgrund dessen das ESM-Gerät ersetzt werden muss. Wenn die Kommunikationsinformationen vor dem Fehler nicht exportiert wurden, kann die Kommunikation mit dem Gerät nicht wiederhergestellt werden. Bei dieser Methode wird die PRK-Datei exportiert und importiert.

Der private Schlüssel für das primäre ESM-Gerät wird vom sekundären ESM-Gerät verwendet, um anfangs die Kommunikation mit dem Gerät herzustellen. Wenn die Kommunikation hergestellt ist, wird der öffentliche Schlüssel des sekundären ESM-Geräts in die Tabelle der autorisierten Schlüssel für das Gerät kopiert. Anschließend wird auf dem sekundären ESM-Gerät der private Schlüssel für das primäre ESM-Gerät gelöscht und die Kommunikation mit dem eigenen öffentlichen oder privaten Schlüsselpaar initiiert.

Aktion	Schritte
Exportieren der PRK-Datei vom primären ESM-Gerät	1 Wählen Sie in der Systemnavigationsstruktur des primären ESM-Geräts das Gerät mit den zu sichernden Kommunikationsinformationen aus, und klicken Sie dann auf das Symbol **Eigenschaften**. 2 Wählen Sie **Schlüsselverwaltung** aus, und klicken Sie dann auf **Schlüssel exportieren**. 3 Wählen Sie **Privaten SSH-Schlüssel sichern** aus, und klicken Sie dann auf **Weiter**. 4 Geben Sie ein Kennwort ein, bestätigen Sie es, und legen Sie dann das Ablaufdatum fest. Wenn das Ablaufdatum verstrichen ist, kann die Person, die den Schlüssel importiert, erst mit dem Gerät kommunizieren, wenn ein anderer Schlüssel mit einem in der Zukunft liegenden Ablaufdatum exportiert wird. Wenn Sie **Kein Ablauf** auswählen und der Schlüssel auf einem anderen ESM-Gerät importiert wird, läuft der Schlüssel nie ab. 5 Klicken Sie auf **OK**, wählen Sie den Speicherort für die vom ESM-Gerät erstellte PRK-Datei aus, und melden Sie sich dann beim primären ESM-Gerät ab.
Hinzufügen eines Geräts zum sekundären ESM-Gerät und Importieren der PRK-Datei	1 Wählen Sie in der Systemnavigationsstruktur des sekundären Geräts das System oder den Knoten auf Gruppenebene aus, zu dem Sie das Gerät hinzufügen möchten. 2 Klicken Sie auf der Aktionssymbolleiste auf **Gerät hinzufügen**. 3 Wählen Sie den Typ des hinzuzufügenden Geräts aus, und klicken Sie dann auf **Weiter**. 4 Geben Sie einen in dieser Gruppe eindeutigen Namen für das Gerät ein, und klicken Sie dann auf **Weiter**. 5 Geben Sie die Ziel-IP-Adresse des Geräts ein, geben Sie den FIPS-Kommunikationsport ein, und klicken Sie dann auf **Weiter**. 6 Klicken Sie auf **Schlüssel importieren**, navigieren Sie zu der zuvor exportierten PRK-Datei, und klicken Sie dann auf **Hochladen**. Geben Sie das Kennwort ein, das Sie beim anfänglichen Export des Schlüssels festgelegt haben. 7 Melden Sie sich beim sekundären ESM-Gerät ab.

Aktivieren der Kommunikation mit mehreren ESM-Geräten im FIPS-Modus

Sie können die Kommunikation zwischen mehreren ESM-Geräten und dem gleichen Gerät zulassen, indem Sie PUK- und EXK-Dateien exportieren und importieren.

Bei dieser Methode werden zwei Export- und Importprozesse verwendet. Zuerst wird über das primäre ESM-Gerät die vom sekundären ESM-Gerät exportierte PUK-Datei importiert und der darin enthaltene öffentliche Schlüssel des sekundären ESM-Geräts an das Gerät gesendet. Anschließend ist die Kommunikation zwischen beiden ESM-Geräten und dem Gerät möglich. Im zweiten Schritt wird die EXK-Datei des Geräts vom primären ESM-Gerät exportiert und auf dem sekundären ESM-Gerät importiert. Damit wird dem sekundären ESM-Gerät die Kommunikation mit dem Gerät ermöglicht.

Aktion	Schritte
Exportieren der PUK-Datei vom sekundären ESM-Gerät	1 Wählen Sie auf der Seite **Systemeigenschaften** des sekundären ESM-Geräts die Option **ESM-Verwaltung** aus. 2 Klicken Sie auf **SSH exportieren**, und wählen Sie dann den Speicherort für die PUK-Datei aus. 3 Klicken Sie auf **Speichern**, und melden Sie sich dann ab.
Importieren der PUK-Datei auf dem primären ESM-Gerät	1 Wählen Sie in der Systemnavigationsstruktur des primären ESM-Geräts das Gerät aus, das Sie konfigurieren möchten. 2 Klicken Sie auf das Symbol **Eigenschaften**, und wählen Sie dann **Schlüsselverwaltung** aus. 3 Klicken Sie auf **SSH-Schlüssel verwalten**. 4 Klicken Sie auf **Importieren**, wählen Sie die PUK-Datei aus, und klicken Sie dann auf **Hochladen**. 5 Klicken Sie auf **OK**, und melden Sie sich dann beim primären ESM-Gerät ab.

Aktion	Schritte
Exportieren der EXK-Datei des Geräts vom primären ESM-Gerät	1 Wählen Sie in der Systemnavigationsstruktur des primären ESM-Geräts das Gerät aus, das Sie konfigurieren möchten. 2 Klicken Sie auf das Symbol **Eigenschaften**, und wählen Sie dann **Schlüsselverwaltung** aus. 3 Klicken Sie auf **Schlüssel exportieren**, wählen Sie den gesicherten Geräteschlüssel aus, und klicken Sie dann auf **Weiter**. 4 Geben Sie ein Kennwort ein, bestätigen Sie es, und legen Sie dann das Ablaufdatum fest. Wenn das Ablaufdatum verstrichen ist, kann die Person, die den Schlüssel importiert, erst mit dem Gerät kommunizieren, wenn ein anderer Schlüssel mit einem in der Zukunft liegenden Ablaufdatum exportiert wird. Wenn Sie **Kein Ablauf** auswählen und der Schlüssel auf einem anderen ESM-Gerät importiert wird, läuft der Schlüssel nie ab. 5 Wählen Sie die Berechtigungen für die EXK-Datei aus, und klicken Sie dann auf **OK**. 6 Wählen Sie den Speicherort für die Datei aus, und melden Sie sich dann beim primären ESM-Gerät ab.
Importieren der EXK-Datei auf dem sekundären ESM-Gerät	1 Wählen Sie in der Systemnavigationsstruktur des sekundären Geräts das System oder den Knoten auf Gruppenebene aus, zu dem Sie das Gerät hinzufügen möchten. 2 Klicken Sie auf der Aktionssymbolleiste auf **Gerät hinzufügen**. 3 Wählen Sie den Typ des hinzuzufügenden Geräts aus, und klicken Sie dann auf **Weiter**. 4 Geben Sie einen in dieser Gruppe eindeutigen Namen für das Gerät ein, und klicken Sie dann auf **Weiter**. 5 Klicken Sie auf **Schlüssel importieren**, und wechseln Sie dann zur EXK-Datei. 6 Klicken Sie auf **Hochladen**, und geben Sie dann das beim Exportieren des Schlüssels festgelegte Kennwort ein. 7 Melden Sie sich beim sekundären ESM-Gerät ab.

Fehlerbehebung für den FIPS-Modus

Beim Betrieb des ESM-Geräts im FIPS-Modus kann es zu Problemen kommen.

Problem	Beschreibung und Behebung
Keine Kommunikation mit dem ESM-Gerät	• Überprüfen Sie das LCD-Display auf der Vorderseite des Geräts. Wenn dort **FIPS-Fehler** angezeigt wird, wenden Sie sich an den McAfee-Support. • Überprüfen Sie über die HTTP-Schnittstelle, ob eine Fehlerbedingung vorliegt. Zeigen Sie dazu in einem Browser die ESM-Webseite für den FIPS-Selbsttest an. – Wenn die einzelne Ziffer **0** angezeigt wird, die auf das Fehlschlagen eines FIPS-Selbsttests hinweist, starten Sie das ESM-Gerät neu, und versuchen Sie, das Problem zu beheben. Wenn die Fehlerbedingung weiterhin besteht, wenden Sie sich an den Support, und bitten Sie um weitere Anweisungen. – Wenn die einzelne Ziffer **1** angezeigt wird, ist das Kommunikationsproblem nicht auf einen FIPS-Fehler zurückzuführen. Wenden Sie sich an den Support, und erkundigen Sie sich nach weiteren Schritten zur Fehlerbehebung.
Keine Kommunikation mit dem Gerät	• Wenn neben dem Gerät in der Systemnavigationsstruktur eine Statuskennzeichnung angezeigt wird, platzieren Sie den Cursor auf der Kennzeichnung. Wenn dort **FIPS-Fehler** angezeigt wird, wenden Sie sich über das Support-Portal an den McAfee-Support. • Folgen Sie der Beschreibung für das Problem *Keine Kommunikation mit dem ESM-Gerät*.
Fehlermeldung **Die Datei ist ungültig** beim Hinzufügen eines Geräts	Sie können nicht einen von einem Nicht-FIPS-Gerät exportierten Schlüssel auf einem im FIPS-Modus betriebenen Gerät importieren. Ebenso ist es nicht möglich, einen von einem FIPS-Gerät exportierten Schlüssel auf einem Nicht-FIPS-Gerät zu importieren. In beiden Szenarien wird diese Fehlermeldung angezeigt.

Zertifizierte Common Criteria-Konfiguration

Sie müssen die McAfee-Appliance auf eine bestimmte Weise installieren, konfigurieren und verwenden, um Compliance mit der zertifizierten Common Criteria-Konfiguration zu erzielen. Berücksichtigen Sie diese Anforderungen beim Einrichten des Systems.

Typ	Anforderungen
Physisch	Auf die McAfee-Appliance muss Folgendes zutreffen: • Sie muss vor nicht autorisierten physischen Änderungen geschützt sein. • Sie muss sich in einer Einrichtung mit Zugriffssteuerung befinden, in der kein nicht autorisierter physischer Zugriff möglich ist.
Beabsichtigte Verwendung	Auf die McAfee-Appliance muss Folgendes zutreffen: • Sie muss Zugriff auf den gesamten Netzwerkverkehr haben, damit ihre Funktionen ausgeführt werden können. • Sie muss so verwaltet werden, dass Adressenänderungen in dem vom Target of Evaluation (TOE) überwachten Netzwerkverkehr möglich sind. • Sie muss für den überwachten Netzwerkverkehr skaliert werden.

Typ	Anforderungen
Personal	• Für die Verwaltung der McAfee-Appliance und der Sicherheit der darin enthaltenen Informationen muss mindestens eine fachkundige Person zugewiesen sein. Vor-Ort-Unterstützung bei der Installation und Konfiguration sowie Vor-Ort-Schulung für die Verwendung der Appliance wird von McAfee-Technikern für alle McAfee-Kunden bereitgestellt. • Die autorisierten Administratoren verhalten sich nicht nachlässig, vorsätzlich fahrlässig oder ablehnend und halten sich an die Anweisungen in der Dokumentation für die McAfee-Appliance. • Nur autorisierte Benutzer dürfen auf die McAfee-Appliance zugreifen. • Die für die McAfee-Appliance zuständigen Personen müssen sicherstellen, dass alle Anmeldeinformationen für den Zugriff von den Benutzern im Hinblick auf die IT-Sicherheit geschützt werden.
Sonstige	• Wenden Sie keine Software-Aktualisierungen auf die McAfee-Appliance an, da sich dadurch eine von der Common Criteria-Konfiguration abweichende Konfiguration ergibt. Zertifizierte Aktualisierungen erhalten Sie vom McAfee-Support. • Wenn Sie für ein Nitro IPS-Gerät die Einstellungen **Watchdog-Timer** und **Umgehung erzwingen** auf der Seite **Einstellungen für Netzwerkschnittstellen** aktivieren, ergibt sich eine von der zertifizierten Common Criteria-Konfiguration abweichende Konfiguration. • Wenn Sie bei einem Nitro IPS-Gerät für den Überbelegungsmodus eine andere Einstellung als **Verwerfen** verwenden, ergibt sich eine von der zertifizierten Common Criteria-Konfiguration abweichende Konfiguration. • Wenn Sie die Funktion **Anmeldesicherheit** mit einem RADIUS-Server aktivieren, ergibt sich sichere Kommunikation. Die IT-Umgebung ermöglicht die sichere Übertragung von Daten zwischen dem TOE und externen Entitäten und Quellen. Externe Authentifizierungsdienste können von einem RADIUS-Server bereitgestellt werden. • Die Verwendung der **Smart Dashboard**-Funktionalität der Check Point-Firewall-Konsole ist nicht Bestandteil des TOE. • Die Verwendung von Snort Barnyard ist nicht Bestandteil des TOE. • Die Verwendung des MEF-Clients ist nicht Bestandteil des TOE. • Die Verwendung des Remedy-Ticket-Systems ist nicht Bestandteil des TOE.

An- und Abmelden

Wenn Sie die Geräte installiert und eingerichtet haben, können Sie sich zum ersten Mal bei der ESM-Konsole anmelden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie auf dem Client-Computer einen Web-Browser, und wechseln Sie zu der IP-Adresse, die Sie beim Konfigurieren der Netzwerkschnittstelle festgelegt haben.

2 Klicken Sie auf **Anmeldung**, wählen Sie die Sprache für die Konsole aus, und geben Sie dann den Standardbenutzernamen und das entsprechende Kennwort ein.

- Standardbenutzername: `NGCP`
- Standardkennwort: `security.4u`

3 Klicken Sie auf **Anmeldung**, lesen Sie den **Endbenutzer-Lizenzvertrag**, und klicken Sie anschließend auf **Akzeptieren**.

4 Ändern Sie den Benutzernamen und das Kennwort, und klicken Sie dann auf **OK**.

5 Wählen Sie aus, ob der FIPS-Modus aktiviert werden soll.

> Wenn Sie im FIPS-Modus arbeiten müssen, müssen Sie diesen bei der ersten Anmeldung beim System aktivieren, damit alle zukünftigen Vorgänge mit McAfee-Geräten im FIPS-Modus stattfinden. Sie sollten den FIPS-Modus nur aktivieren, wenn dies erforderlich ist. Weitere Informationen finden Sie unter *Informationen zum FIPS-Modus*.

6 Folgen Sie den Anweisungen, um den Benutzernamen und das Kennwort zu erhalten, die Sie für den Zugriff auf Regelaktualisierungen benötigen.

7 Führen Sie die Erstkonfiguration von ESM aus:

a Wählen Sie die Sprache aus, die für die Systemprotokolle verwendet werden soll.

b Wählen Sie die Zeitzone für das ESM-Gerät und das Datumsformat für das Konto aus, und klicken Sie dann auf **Weiter**.

c Definieren Sie die Einstellungen auf den Seiten des Assistenten **Erstkonfiguration von ESM**. Klicken Sie auf den einzelnen Seiten auf das Symbol **Hilfe anzeigen**, um Anweisungen anzuzeigen.

8 Klicken Sie auf **OK** und dann auf die Links zu Hilfe bei den ersten Schritten oder zu den neuen Funktionen, die in dieser Version von ESM zur Verfügung stehen.

9 Melden Sie sich nach Abschluss der Arbeitssitzung mit einer der folgenden Methoden ab:

- Wenn keine Seiten geöffnet sind, klicken Sie rechts oben in der Konsole auf der Systemnavigationsleiste auf **Abmelden**.
- Wenn Seiten geöffnet sind, schließen Sie den Browser.

Siehe auch

Informationen zum FIPS-Modus auf Seite 13

Anpassen der Anmeldeseite

Sie können die Anmeldeseite anpassen, indem Sie Text wie beispielsweise Sicherheitsrichtlinien des Unternehmens oder ein Logo hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Optionen **Systemeigenschaften** | **Benutzerdefinierte Einstellungen**.

2 Führen Sie eine oder mehrere der folgenden Aktionen aus:

Aufgabe	Vorgehensweise
Hinzufügen von benutzerdefiniertem Text	1 Klicken Sie oben auf der Seite auf das Textfeld. 2 Geben Sie den Text ein, den Sie zur Seite **Anmeldung** hinzufügen möchten. 3 Wählen Sie **Text in Anmeldebildschirm einschließen** aus.
Hinzufügen eines benutzerdefinierten Bilds	1 Klicken Sie auf **Bild auswählen**. 2 Laden Sie das Bild hoch, das Sie verwenden möchten. 3 Wählen Sie **Bild in Anmeldebildschirm einschließen** aus. Wenn nach dem Hochladen eines neuen benutzerdefinierten Logos auf der Seite **Anmeldung** noch das alte Logo angezeigt wird, löschen Sie den Cache des Browsers.
Löschen eines benutzerdefinierten Bilds	Klicken Sie auf **Bild löschen**. Das Standardlogo wird angezeigt.

Aktualisieren der ESM-Software

Greifen Sie auf Software-Aktualisierungen vom Aktualisierungs-Server oder von einem Sicherheitsmitarbeiter zu, und laden Sie diese dann in das ESM-Gerät hoch.

Informationen zum Aktualisieren eines primären oder redundanten ESM-Geräts finden Sie unter *Aktualisieren eines primären oder redundanten ESM-Geräts*.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **ESM-Verwaltung**.

2 Klicken Sie auf der Registerkarte **Wartung** auf **ESM aktualisieren**.

3 Wählen Sie die Datei aus, die Sie zum Aktualisieren des ESM-Geräts verwenden möchten, und klicken Sie dann auf **OK**.

Das ESM-Gerät wird neu gestartet, und alle aktuellen Sitzungen werden während der Installation der Aktualisierung getrennt.

Siehe auch

Aktualisieren eines primären oder redundanten ESM-Geräts auf Seite 216

Anfordern und Hinzufügen von Anmeldeinformationen für Regelaktualisierungen

Über ESM erhalten Sie im Rahmen Ihres Wartungsvertrags Aktualisierungen für Richtlinien, Parser und Regeln. Sie können 30 Tage lang ohne dauerhafte Anmeldeinformationen auf ESM zugreifen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Fordern Sie die Anmeldeinformationen per E-Mail von Licensing@McAfee.com an. Geben Sie dabei die folgenden Informationen an:
   - McAfee-Grant-Nummer
   - Kontoname
   - Adresse
   - Kontaktname
   - E-Mail-Adresse
2. Wenn Sie die Kunden-ID und das Kennwort von McAfee erhalten haben, wählen Sie in der Systemnavigationsstruktur die Optionen **Systemeigenschaften** | **Systeminformationen** | **Regelaktualisierung** aus.
3. Klicken Sie auf **Anmeldeinformationen**, und geben Sie dann die Kunden-ID und das Kennwort ein.
4. Klicken Sie auf **Überprüfen**.

Überprüfen auf Regelaktualisierungen

Die von einem Nitro IPS-Gerät oder einem virtuellen Gerät für die Untersuchung des Netzwerkverkehrs verwendeten Regelsignaturen werden vom für Signaturen zuständigen McAfee-Team ständig aktualisiert und können vom zentralen Server von McAfee heruntergeladen werden. Die Regelaktualisierungen können automatisch oder manuell abgerufen werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und vergewissern Sie sich, dass **Systeminformationen** ausgewählt ist.
2. Vergewissern Sie sich im Feld **Regelaktualisierungen**, dass Ihre Lizenz nicht abgelaufen ist.

   Wenn die Lizenz abgelaufen ist, finden Sie weitere Informationen unter *Anfordern und Hinzufügen von Anmeldeinformationen für Regelaktualisierungen*.
3. Wenn die Lizenz gültig ist, klicken Sie auf **Regelaktualisierung**.
4. Wählen Sie eine der folgenden Optionen aus:
   - Mit **Intervall für automatische Überprüfung** richten Sie das System so ein, dass mit der ausgewählten Häufigkeit automatisch eine Überprüfung auf Aktualisierungen vorgenommen wird.
   - Mit **Jetzt überprüfen** führen Sie die Überprüfung auf Aktualisierungen sofort aus.
   - Mit **Manuelle Aktualisierung** aktualisieren Sie die Regeln aus einer lokalen Datei.
5. Klicken Sie auf **OK**.

Siehe auch

Anfordern und Hinzufügen von Anmeldeinformationen für Regelaktualisierungen auf Seite 23

Ändern der Sprache für Ereignisprotokolle

Bei der ersten Anmeldung beim ESM-Gerät haben Sie die Sprache für Ereignisprotokolle wie beispielsweise das Protokoll der Integritätsüberwachung und das Geräteprotokoll ausgewählt. Sie können diese Spracheinstellung ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur Folgendes aus: **Systemeigenschaften** | **ESM-Verwaltung**.

2 Klicken Sie auf **Gebietsschema des Systems**, wählen Sie in der Dropdown-Liste eine Sprache aus, und klicken Sie dann auf **OK**.

Verbinden von Geräten

Verbinden Sie physische und virtuelle Geräte mit McAfee ESM, um forensische Funktionen in Echtzeit, Anwendungs- und Datenbanküberwachung, erweiterte regel- und risikobasierte Korrelation sowie die Erstellung von Compliance-Berichten zu ermöglichen.

Wenn mehr Geräte zum System hinzukommen, sollten Sie sie logisch anordnen. Wenn Sie beispielsweise Niederlassungen an verschiedenen Orten haben, zeigen Sie die entsprechenden Geräte nach der jeweiligen Zone an. Sie können die vordefinierten Anzeigen verwenden oder eigene benutzerdefinierte Anzeigen entwerfen. Sie können die Geräte weiter untergliedern, indem Sie in den einzelnen benutzerdefinierten Anzeigen Gruppen hinzufügen.

Inhalt

- *Hinzufügen von Geräten zur ESM-Konsole*
- *Auswählen eines Anzeigetyps*
- *Verwalten benutzerdefinierter Anzeigetypen*
- *Verwalten einer Gruppe in einem benutzerdefinierten Anzeigetyp*
- *Löschen einer Gruppe oder eines Geräts*
- *Löschen doppelter Geräte in der Systemnavigationsstruktur*

Hinzufügen von Geräten zur ESM-Konsole

Wenn Sie physische und virtuelle Geräte eingerichtet und installiert haben, müssen Sie diese zur ESM-Konsole hinzufügen.

> **Bevor Sie beginnen**
>
> Richten Sie die Geräte ein, und installieren Sie sie (siehe *McAfee Enterprise Security Manager – Installationshandbuch*).

Vorgehensweise

1 Klicken Sie in der Systemnavigationsstruktur auf **Lokales ESM-Gerät** oder auf eine Gruppe.

2 Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Gerät hinzufügen**  .

3 Wählen Sie den Typ des hinzuzufügenden Geräts aus, und klicken Sie dann auf **Weiter**.

4 Gegeben Sie im Feld **Gerätename** einen in der Gruppe eindeutigen Namen ein, und klicken Sie dann auf **Weiter**.

5 Geben Sie die erforderlichen Informationen ein:

- Für McAfee ePO-Geräte: Wählen Sie einen Empfänger aus, geben Sie die erforderlichen Anmeldeinformationen für die Anmeldung bei der Web-Oberfläche ein, und klicken Sie dann auf **Weiter**. Geben Sie die Einstellungen ein, die für die Kommunikation mit der Datenbank verwendet werden sollen.

  Wählen Sie **Benutzerauthentifizierung erforderlich** aus, um den Zugriff auf die Benutzer zu begrenzen, die über den Benutzernamen und das Kennwort für das Gerät verfügen.

- Für alle anderen Geräte: Geben Sie die Ziel-IP-Adresse oder URL für das Gerät ein. Geben Sie dann eine Nummer eines Ziel-SSH-Ports ein, die für die Verwendung mit der IP-Adresse gültig ist.

6 Wählen Sie aus, ob die NTP-Einstellungen (Network Time Protocol) auf dem Gerät verwendet werden sollen, und klicken Sie dann auf **Weiter**.

7 Wenn Sie einen Schlüssel haben, den Sie importieren möchten, wählen Sie **Schlüssel importieren** aus (nicht verfügbar für ELM oder Kombination aus Empfänger und Log Manager). Anderenfalls klicken Sie auf **Authentifizierungsschlüssel für Gerät festlegen**.

Geräteschlüssel, die ursprünglich von einem ESM-Gerät mit einer niedrigeren Version als 8.3.X exportiert wurden, verfügen nicht über Informationen zum Kommunikationsmodell der Version 8.4.0. Beim Durchführen des Upgrades mussten Sie den Authentifizierungsschlüssel für das Gerät erneut festlegen. Um Zugriff auf Geräte mit Version 9.0.0 oder höher zu erhalten, müssen Sie den Schlüssel für dieses Gerät von einem ESM-Gerät mit Version 8.5.0 oder höher erneut exportieren. Achten Sie darauf, alle für das Gerät erforderlichen Berechtigungen festzulegen, beispielsweise die Berechtigung **Virtuelle Geräte konfigurieren**.

8 Geben Sie ein Kennwort für das Gerät ein, und klicken Sie dann auf **Weiter**.

Die Kommunikation zwischen dem ESM-Gerät und dem anderen Gerät wird getestet, und der Verbindungsstatus wird gemeldet.

Auswählen eines Anzeigetyps

Wählen Sie aus, wie die Geräte in der Systemnavigationsstruktur angezeigt werden sollen.

Bevor Sie beginnen

Zum Auswählen einer benutzerdefinierten Anzeige müssen Sie diese zuerst zum System hinzufügen (siehe *Verwalten benutzerdefinierter Anzeigetypen*).

Vorgehensweise

1 Klicken Sie im Systemnavigationsbereich auf den Dropdown-Pfeil im Feld für den Anzeigetyp.

2 Wählen Sie einen der Anzeigetypen aus.

Die Anordnung der Geräte in der Navigationsstruktur wird geändert und entspricht nun dem Typ, den Sie für die aktuelle Arbeitssitzung ausgewählt haben.

Verwalten benutzerdefinierter Anzeigetypen

Sie können die Anordnung der Geräte in der Systemnavigationsstruktur definieren, indem Sie benutzerdefinierte Anzeigetypen hinzufügen, bearbeiten oder löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Systemnavigationsbereich auf den Dropdown-Pfeil für den Anzeigetyp.

2 Führen Sie einen der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Hinzufügen eines benutzerdefinierten Anzeigetyps	1 Klicken Sie auf **Anzeige hinzufügen**. 2 Füllen Sie die Felder aus, und klicken Sie dann auf **OK**.
Bearbeiten eines benutzerdefinierten Anzeigetyps	1 Klicken Sie neben dem zu bearbeitenden Anzeigetyp auf das Symbol **Bearbeiten**. 2 Nehmen Sie Änderungen an den Einstellungen vor, und klicken Sie dann auf **OK**.
Löschen eines benutzerdefinierten Anzeigetyps	Klicken Sie neben dem zu löschenden Anzeigetyp auf das Symbol **Löschen**.

Verwalten einer Gruppe in einem benutzerdefinierten Anzeigetyp

Sie können Gruppen in einem benutzerdefinierten Anzeigetyp verwenden, um Geräte in logischen Gruppierungen anzuordnen.

Bevor Sie beginnen

Fügen Sie einen benutzerdefinierten Anzeigetyp hinzu (siehe *Verwalten benutzerdefinierter Anzeigetypen*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Systemnavigationsbereich auf die Dropdown-Liste für den Anzeigetyp.

2 Wählen Sie die benutzerdefinierte Anzeige aus, und führen Sie dann einen der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Hinzufügen einer neuen Gruppe	1 Klicken Sie auf einen System- oder Gruppenknoten und dann auf der Aktionssymbolleiste auf das Symbol **Gruppe hinzufügen**. 2 Füllen Sie die Felder aus, und klicken Sie dann auf **OK**. 3 Ziehen Sie Geräte in der Anzeige an die gewünschte Stelle, und legen Sie sie ab, um sie zur Gruppe hinzuzufügen. Wenn das Gerät Teil einer Struktur in der Anzeige ist, wird ein doppelter Geräteknoten erstellt. Das Duplikat in der Systemstruktur können Sie anschließend löschen.
Bearbeiten einer Gruppe	Wählen Sie die Gruppe aus, klicken Sie auf das Symbol **Eigenschaften**, und nehmen Sie dann auf der Seite **Gruppeneigenschaften** Änderungen vor.
Löschen einer Gruppe	Wählen Sie die Gruppe aus, und klicken Sie dann auf das Symbol **Gruppe löschen**. Die Gruppe und die darin enthaltenen Geräte werden aus der benutzerdefinierten Anzeige gelöscht. Die Geräte werden nicht aus dem System gelöscht.

Siehe auch

Verwalten benutzerdefinierter Anzeigetypen auf Seite 26

Löschen einer Gruppe oder eines Geräts

Wenn ein Gerät nicht mehr Bestandteil des Systems ist oder Sie eine Gruppe nicht mehr verwenden, löschen Sie das Gerät bzw. die Gruppe aus der Systemnavigationsstruktur.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Heben Sie in der Systemnavigationsstruktur das zu löschende Gerät bzw. die zu löschende Gruppe hervor, und klicken Sie dann auf der Aktionssymbolleiste auf das Symbol **Löschen**.

2 Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **OK**.

Löschen doppelter Geräte in der Systemnavigationsstruktur

Doppelte Geräteknoten werden in der Systemnavigationsstruktur angezeigt, wenn Sie Geräte aus einer Systemstruktur in eine Gruppe ziehen und dort ablegen oder wenn Gruppen eingerichtet sind und Sie dann ein Upgrade der ESM-Software durchführen. Es wird empfohlen, die doppelten Geräteknoten zu löschen, um Verwirrung zu vermeiden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Systemnavigationsbereich auf die Dropdown-Liste für den Anzeigetyp.

2 Wählen Sie das Symbol **Bearbeiten** neben der Anzeige mit den doppelten Geräten aus.

3 Heben Sie die Auswahl der doppelten Geräte auf, und klicken Sie dann auf **OK**.

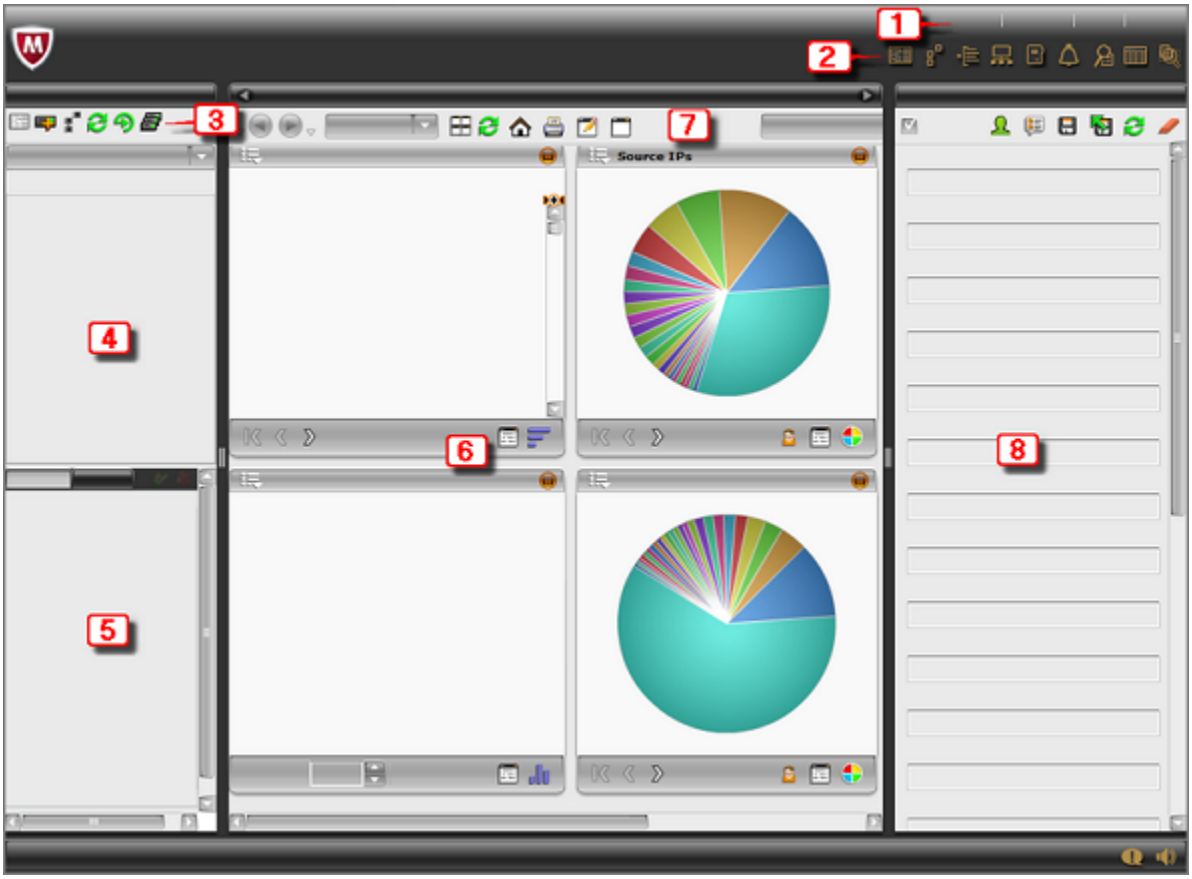
Die Geräte, für die Duplikate vorhanden waren, werden jetzt nur in den zugewiesenen Gruppen aufgeführt.

Konsoleneinstellungen

Sie können verschiedene Funktionen der ESM-Konsole anpassen, indem Sie das Farbdesign, das Format für Datum und Uhrzeit, den Zeitüberschreitungswert und verschiedene Standardeinstellungen ändern. Außerdem können Sie Anmeldeinformationen für McAfee® ePolicy Orchestrator® (McAfee ePO™) einrichten.

ESM-Konsole

In der ESM-Konsole erhalten Sie nahezu in Echtzeit Einblicke in Ihre Geräte und können schnell auf Alarmbenachrichtigungen und zugewiesene Fälle zugreifen.



1 **Systemnavigationsleiste** für allgemeine Setup-Funktionen

2 **Symbole** für den Zugriff auf häufig verwendete Seiten

3 **Aktionssymbolleiste** zum Auswählen der notwendigen Funktionen zum Konfigurieren der einzelnen Geräte

4 **Systemnavigationsbereich** zum Anzeigen der Geräte im System

5 **Bereich für Alarme und Fälle** zum Anzeigen von Alarmbenachrichtigungen und zugewiesenen offenen Fällen

6 **Ansichtsbereich** für Ereignis-, Fluss- und Protokolldaten

7 **Ansichtssymbolleiste** zum Erstellen, Bearbeiten und Verwalten von Ansichten

8 **Filterbereich** zum Anwenden von Filtern auf ereignis- oder flussbasierte Datenansichten

Arbeiten mit dem Farbdesign für die Konsole

Passen Sie die ESM-Konsole an, indem Sie ein vorhandenes Farbdesign auswählen oder ein eigenes entwerfen. Sie können auch benutzerdefinierte Farbdesigns bearbeiten oder löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf der Systemnavigationsleiste der ESM-Konsole auf **Optionen**.
2. Sie können ein vorhandenes Farbdesign auswählen oder ein benutzerdefiniertes Design hinzufügen, bearbeiten oder entfernen.
3. Wenn Sie auf **Hinzufügen** oder **Bearbeiten** klicken, wählen Sie die Farben für das benutzerdefinierte Design aus, und klicken Sie dann auf **OK**.

   Wenn Sie ein neues Design hinzugefügt haben, wird im Abschnitt **Wählen Sie ein Design aus** ein Miniaturbild mit Ihren Farben angezeigt.
4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Auswählen von Einstellungen für die Konsolenansicht

Legen Sie die Standardeinstellungen für die Ansichten in der ESM-Konsole fest.

Auf dieser Seite können Sie die folgenden Aktionen für das System festlegen:

- Automatisches Aktualisieren der Daten in einer geöffneten Ansicht
- Ändern der Ansichten, die beim Starten des Systems standardmäßig geöffnet werden
- Ändern der Ansichten, die beim Auswählen von **Zusammenfassen** in einer Ereignis- oder Flussansicht geöffnet werden

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf der Systemnavigationsleiste der ESM-Konsole auf **Optionen**.
2. Wählen Sie auf der Seite **Ansichten** die Einstellungen aus, und klicken Sie dann auf **OK**.

Festlegen des Zeitüberschreitungswerts für die Konsole

Die aktuelle Sitzung in der ESM-Konsole bleibt geöffnet, solange Aktivitäten stattfinden. Legen Sie fest, wie viel Zeit ohne Aktivität verstreichen kann, bis die Sitzung geschlossen wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Optionen **Systemeigenschaften** | **Anmeldesicherheit**.
2. Wählen Sie in **Zeitüberschreitungswert für Benutzeroberfläche** aus, wie viele Minuten ohne Aktivitäten verstreichen müssen. Klicken Sie dann auf **OK**.

   Wenn Sie Null (0) auswählen, bleibt die Konsole unbegrenzt geöffnet.

Auswählen von Benutzereinstellungen

Auf der Seite **Benutzereinstellungen** können Sie verschiedene Standardeinstellungen ändern. Sie können die Zeitzone, das Datumsformat, das Kennwort, die Standardanzeige und die Sprache der Konsole

ändern. Außerdem können Sie auswählen, ob deaktivierte Datenquellen und die Registerkarten **Alarme** und **Fälle** angezeigt werden sollen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf der Systemnavigationsleiste der ESM-Konsole auf **Optionen**.
2. Vergewissern Sie sich, dass **Benutzereinstellungen** ausgewählt ist.
3. Nehmen Sie nach Bedarf Änderungen an den Einstellungen vor, und klicken Sie dann auf **OK**.

Die Darstellung der Konsole wird basierend auf den Einstellungen geändert.

Einrichten von Benutzeranmeldeinformationen für McAfee ePO

Sie können den Zugriff auf ein McAfee ePO-Gerät begrenzen, indem Sie Benutzeranmeldeinformationen festlegen.

Bevor Sie beginnen

Das McAfee ePO-Gerät darf nicht so eingerichtet werden, dass globale Benutzerauthentifizierung erforderlich ist (siehe **Einrichten der globalen Benutzerauthentifizierung**).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf der Systemnavigationsleiste der ESM-Konsole auf **Optionen**, und wählen Sie dann **ePO-Anmeldeinformationen** aus.
2. Klicken Sie auf das Gerät und dann auf **Bearbeiten**.



Wenn in der Statusspalte für das Gerät **Nicht erforderlich** angezeigt wird, ist das Gerät für globale Benutzerauthentifizierung eingerichtet. Sie können den Status auf der Seite **Verbindung** für das Gerät ändern (siehe *Ändern der Verbindung mit ESM*).

3. Geben Sie den Benutzernamen und das Kennwort ein, testen Sie die Verbindung, und klicken Sie dann auf **OK**.

Für den Zugriff auf dieses Gerät benötigen Benutzer den Benutzernamen und das Kennwort, die Sie hinzugefügt haben.

3 Konfigurieren von ESM

Mit ESM werden Daten, Einstellungen, Aktualisierungen und Konfigurationen verwaltet. Die Kommunikation erfolgt mit mehreren Geräten gleichzeitig. Wägen Sie beim Erstellen der ESM-Umgebung sorgfältig die Anforderungen des Unternehmens und die Compliance-Ziele ab, die den Sicherheitsverwaltungs-Lebenszyklus im Unternehmen unterstützen sollen.

Inhalt

- *Verwalten von Geräten*
- *Konfigurieren von Geräten*
- *Konfigurieren von zusätzlichen Diensten*
- *Verwalten der Datenbank*
- *Arbeiten mit Benutzern und Gruppen*
- *Sichern und Wiederherstellen von Systemeinstellungen*
- *Verwalten des ESM-Geräts*
- *Verwenden einer globalen Blacklist*
- *Was ist Datenanreicherung?*

Verwalten von Geräten

Im Systemnavigationsbereich werden die Geräte aufgeführt, die zum System hinzugefügt wurden. Sie können Funktionen für ein oder mehrere Geräte ausführen und die Geräte nach Bedarf anordnen.

Darüber hinaus können Sie, wenn Systeme gekennzeichnet sind, Berichte zum Integritätsstatus anzeigen und vorhandene Probleme beheben.

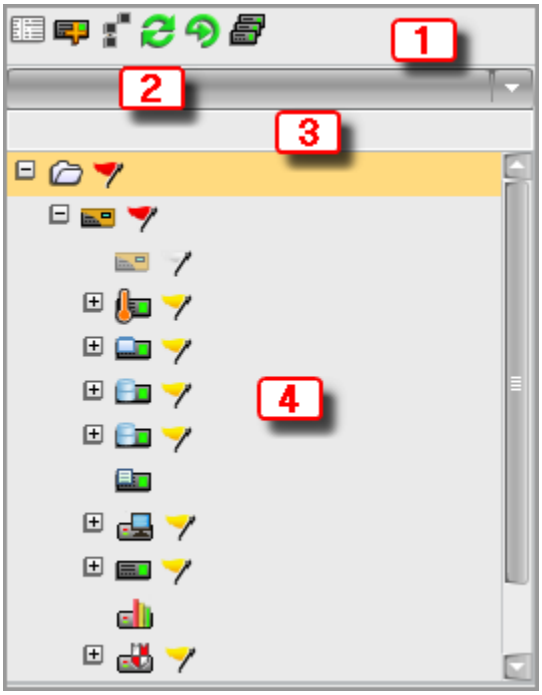


Tabelle 3-1 Funktionsbeschreibungen

Funktion	Zweck
1 Aktionssymbolleiste	Wählen Sie eine Aktion aus, die für Geräte in der Systemnavigationsstruktur ausgeführt werden soll.
Symbol Eigenschaften	Konfigurieren Sie Einstellungen für das in der Systemnavigationsstruktur ausgewählte System oder Gerät.
Symbol Gerät hinzufügen	Fügen Sie Geräte zur Systemnavigationsstruktur hinzu.
Kennzeichnungen für den Integritätsstatus	Zeigen Sie Statuswarnungen für Geräte an.
Verwaltung mehrerer Geräte	Hiermit können Sie mehrere Geräte einzeln starten, anhalten, neu starten und aktualisieren.
Ereignisse und Flüsse abrufen	Rufen Sie Ereignisse und Flüsse für ausgewählte Geräte ab.
Gerät löschen	Löschen Sie das ausgewählte Gerät.
Aktualisieren	Aktualisieren Sie die Daten für alle Geräte.

Tabelle 3-1 Funktionsbeschreibungen *(Fortsetzung)*

Funktion	Zweck
2 Anzeigetyp	Wählen Sie aus, wie die Geräte in der Struktur angeordnet werden sollen. Im Lieferumfang des ESM-Geräts sind drei vordefinierte Typen enthalten: • **Physische Anzeige**: Die Geräte werden hierarchisch aufgeführt. Auf der ersten Ebene befinden sich die Systemknoten (physische Anzeige, lokales ESM-Gerät und lokales ESM-Basisgerät). Auf der zweiten Ebene befinden sich einzelne Geräte und auf allen anderen Ebenen die Quellen, die Sie zu den Geräten hinzufügen (Datenquelle, virtuelles Gerät und andere). Basisgeräte werden automatisch unter den Knoten für lokale ESM-Geräte, Datenquellen, virtuelle Geräte und Datenbank-Server hinzugefügt. Sie sind mit einem abgeblendeten Symbol und Klammern versehen. • **Gerätetyp der Anzeige**: Die Geräte sind nach dem Gerätetyp gruppiert (Nitro IPS, ADM, DEM). • **Zone der Anzeige**: Die Geräte sind nach der Zone angeordnet, die Sie mit der Funktion **Zonenverwaltung** definieren. Sie können auch benutzerdefinierte Anzeigetypen hinzufügen (siehe *Anordnen der Geräte*).
3 Schnellsuche	Führen Sie eine Schnellsuche für ein Gerät in der Systemnavigationsstruktur aus.
4 Systemnavigationsstruktur	Zeigen Sie die Geräte im System an.

Siehe auch
Anordnen der Geräte auf Seite 39
Berichte zum Integritätsstatus von Geräten auf Seite 57
Verwalten mehrerer Geräte auf Seite 56

Anzeigen der Gerätestatistik

Zeigen Sie gerätespezifische Details zu CPU, Arbeitsspeicher und Warteschlange sowie andere gerätespezifische Details an.

Bevor Sie beginnen
Vergewissern Sie sich, dass Sie über die Berechtigung zur Geräteverwaltung verfügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das entsprechende Gerät aus, und klicken Sie dann auf das Symbol Eigenschaften  .

2 Navigieren Sie durch die Optionen und Registerkarten zu **Statistik anzeigen**.

3 Klicken Sie auf **Statistik anzeigen**.

Die Statistik für das Gerät wird in einem Diagramm angezeigt, das alle zehn Minuten aktualisiert wird. Zum Anzeigen von Daten werden Daten von mindestens 30 Minuten benötigt. Jeder Messgrößentyp enthält mehrere Messgrößen, die zum Teil standardmäßig aktiviert sind. Klicken Sie auf **Angezeigt**, um Messgrößen zu aktivieren. In der vierten Spalte wird der Maßstab der entsprechenden Messgröße angezeigt.

Hinzufügen von Geräten zur ESM-Konsole

Wenn Sie physische und virtuelle Geräte eingerichtet und installiert haben, müssen Sie diese zur ESM-Konsole hinzufügen.

Bevor Sie beginnen

Richten Sie die Geräte ein, und installieren Sie sie (siehe *McAfee Enterprise Security Manager – Installationshandbuch*).

Vorgehensweise

1 Klicken Sie in der Systemnavigationsstruktur auf **Lokales ESM-Gerät** oder auf eine Gruppe.

2 Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Gerät hinzufügen**  .

3 Wählen Sie den Typ des hinzuzufügenden Geräts aus, und klicken Sie dann auf **Weiter**.

4 Gegeben Sie im Feld **Gerätename** einen in der Gruppe eindeutigen Namen ein, und klicken Sie dann auf **Weiter**.

5 Geben Sie die erforderlichen Informationen ein:

- Für McAfee ePO-Geräte: Wählen Sie einen Empfänger aus, geben Sie die erforderlichen Anmeldeinformationen für die Anmeldung bei der Web-Oberfläche ein, und klicken Sie dann auf **Weiter**. Geben Sie die Einstellungen ein, die für die Kommunikation mit der Datenbank verwendet werden sollen.

  Wählen Sie **Benutzerauthentifizierung erforderlich** aus, um den Zugriff auf die Benutzer zu begrenzen, die über den Benutzernamen und das Kennwort für das Gerät verfügen.

- Für alle anderen Geräte: Geben Sie die Ziel-IP-Adresse oder URL für das Gerät ein. Geben Sie dann eine Nummer eines Ziel-SSH-Ports ein, die für die Verwendung mit der IP-Adresse gültig ist.

6 Wählen Sie aus, ob die NTP-Einstellungen (Network Time Protocol) auf dem Gerät verwendet werden sollen, und klicken Sie dann auf **Weiter**.

7 Wenn Sie einen Schlüssel haben, den Sie importieren möchten, wählen Sie **Schlüssel importieren** aus (nicht verfügbar für ELM oder Kombination aus Empfänger und Log Manager). Anderenfalls klicken Sie auf **Authentifizierungsschlüssel für Gerät festlegen**.

Geräteschlüssel, die ursprünglich von einem ESM-Gerät mit einer niedrigeren Version als 8.3.X exportiert wurden, verfügen nicht über Informationen zum Kommunikationsmodell der Version 8.4.0. Beim Durchführen des Upgrades mussten Sie den Authentifizierungsschlüssel für das Gerät erneut festlegen. Um Zugriff auf Geräte mit Version 9.0.0 oder höher zu erhalten, müssen Sie den Schlüssel für dieses Gerät von einem ESM-Gerät mit Version 8.5.0 oder höher erneut exportieren. Achten Sie darauf, alle für das Gerät erforderlichen Berechtigungen festzulegen, beispielsweise die Berechtigung **Virtuelle Geräte konfigurieren**.

8 Geben Sie ein Kennwort für das Gerät ein, und klicken Sie dann auf **Weiter**.

Die Kommunikation zwischen dem ESM-Gerät und dem anderen Gerät wird getestet, und der Verbindungsstatus wird gemeldet.

Informationen zu Geräteschlüsseln

Für die Kommunikation zwischen ESM und einem Gerät muss die gesamte Kommunikation mit dem Kommunikationsschlüssel verschlüsselt werden, der beim Festlegen des Schlüssels für das Gerät erstellt wird.

Es wird empfohlen, alle Schlüssel in eine alternative mit einem Kennwort verschlüsselte Datei zu exportieren. Diese können dann importiert werden, um im Notfall die Kommunikation mit einem Gerät wiederherzustellen oder einen Schlüssel auf ein anderes Gerät zu exportieren.

Alle Einstellungen werden auf dem ESM-Gerät gespeichert, das heißt, die ESM-Konsole kennt alle auf dem ESM-Gerät verwalteten Schlüssel. Daher muss ein Geräteschlüssel nicht importiert werden, wenn die Kommunikation zwischen dem ESM-Gerät und dem Gerät bereits erfolgreich stattfindet.

Beispiel: Sie erstellen am Montag eine Sicherung der Einstellungen (einschließlich der Geräteschlüssel) und legen dann am Dienstag den Schlüssel für eines der Geräte erneut fest. Wenn Sie am Mittwoch feststellen, dass Sie die Einstellungen vom Montag wiederherstellen möchten, importieren Sie den Schlüssel, der am Dienstag nach Abschluss der Wiederherstellung der Einstellungen erstellt wurde. Obwohl bei der Wiederherstellung der Geräteschlüssel auf den Stand vom Montag zurückgesetzt wurde, wird auf dem Gerät nur Datenverkehr abgehört, der mit dem Schlüssel vom Dienstag codiert ist. Die Kommunikation mit dem Gerät ist erst nach dem Import des Schlüssels möglich.

Es wird empfohlen, einen Geräteschlüssel nicht auf einem separaten ESM-Gerät zu importieren. Der Exportschlüssel wird verwendet, um ein Gerät im Zusammenhang mit Rollen mit Geräteverwaltungsrechten auf dem verwaltenden ESM-Gerät für das Gerät erneut zu installieren. Wenn Sie ein Gerät auf einem zweiten ESM-Gerät importieren, können verschiedene Gerätefunktionen nicht verwendet werden. Dazu gehören die Richtlinienverwaltung, ELM-Protokollierung und -Verwaltung sowie Einstellungen für Datenquellen und virtuelle Geräte. Geräte-Administratoren können Einstellungen auf dem Gerät von einem anderen ESM-Gerät überschreiben. Es wird empfohlen, ein einziges ESM-Gerät zum Verwalten der mit diesem verbundenen Geräte zu verwenden. Ein DESM-Gerät kann für die Datenerfassung von Geräten, die mit einem anderen ESM-Gerät verbunden sind, verwendet werden.

Festlegen des Schlüssels für ein Gerät

Wenn Sie ein Gerät zum ESM-Gerät hinzugefügt haben, müssen Sie den Schlüssel für das Gerät festlegen, um die Kommunikation zu ermöglichen. Durch das Festlegen des Schlüssels für das Gerät wird die Sicherheit erhöht, da alle externen Kommunikationsquellen ignoriert werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Schlüsselverwaltung** | **Authentifizierungsschlüssel für Gerät festlegen**.

   Wenn die Verbindung vom Gerät hergestellt wurde und die Kommunikation mit dem ESM-Gerät möglich ist, wird der **Assistent für Geräteschlüssel** geöffnet.
3. Geben Sie ein neues Kennwort für das Gerät ein, und klicken Sie dann auf **Weiter**.
4. Klicken Sie auf **Schlüssel exportieren**, und füllen Sie dann die Seite **Schlüssel exportieren** aus, oder klicken Sie auf **Fertig stellen**, wenn Sie den Schlüssel jetzt nicht exportieren möchten.

Exportieren eines Schlüssels

Nach dem Festlegen des Schlüssels für ein Gerät exportieren Sie den Schlüssel in eine Datei.

Wenn Sie das System im FIPS-Modus betreiben, verwenden Sie dieses Verfahren nicht. Das richtige Verfahren finden Sie unter *Hinzufügen eines Geräts mit festgelegtem Schlüssel im FIPS-Modus*.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .
2. Klicken Sie auf **Schlüsselverwaltung** | **Schlüssel exportieren**.
3. Definieren Sie die Einstellungen auf der Seite **Schlüssel exportieren**, und klicken Sie dann auf **OK**.

   Die Datei mit dem Exportschlüssel wird vom ESM-Gerät erstellt, und Sie werden gefragt, ob Sie den Schlüssel exportieren möchten.
4. Klicken Sie auf **Ja**, und wählen Sie dann aus, wo die Datei gespeichert werden soll.

Es wird empfohlen, eine persönliche Sicherungskopie des Geräteschlüssels zu exportieren, die auf **Kein Ablauf** festgelegt ist und alle Berechtigungen enthält.

Importieren eines Schlüssels

Importieren Sie einen Schlüssel, um die vorherigen ESM-Einstellungen wiederherzustellen oder den Schlüssel auf einem anderen ESM-Gerät oder in einer älteren Konsole zu verwenden.

Auf einem Gerät der Version 9.0 oder höher können Sie nur einen Schlüssel von einem ESM-Gerät mit Version 8.5 oder höher importieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .
2. Klicken Sie auf **Schlüsselverwaltung** | **Schlüssel importieren**.
3. Suchen Sie die gespeicherte Schlüsseldatei, und wählen Sie sie aus.
4. Klicken Sie auf **Hochladen**, und geben Sie dann das beim Exportieren des Schlüssels festgelegte Kennwort ein.

Wenn der Schlüssel erfolgreich importiert wurde, wird eine Seite mit dem Status angezeigt.

SSH-Schlüssel verwalten

Geräte können über SSH-Kommunikationsschlüssel für Systeme verfügen, mit denen sichere Kommunikation möglich sein muss. Sie können die Kommunikation mit diesen Systemen anhalten, indem Sie den Schlüssel löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .
2. Klicken Sie auf **Schlüsselverwaltung** und dann auf **SSH-Schlüssel verwalten**.

   Auf der Seite **SSH-Schlüssel verwalten** werden die IDs des ESM-Geräts aufgeführt, mit denen das Gerät kommuniziert.
3. Heben Sie die ID hervor, und klicken Sie auf **Löschen**, um die Kommunikation mit einem der aufgeführten Systeme anzuhalten.
4. Bestätigen Sie den Löschvorgang, und klicken Sie dann auf **OK**.

Aktualisieren der Software eines Geräts

Wenn die Software auf einem Gerät veraltet ist, laden Sie aus einer Datei auf dem ESM-Gerät oder vom lokalen Computer eine neue Version der Software hoch.

Bevor Sie beginnen

Wenn Sie das System seit mehr als 30 Tagen besitzen, müssen Sie sich für den Zugriff auf die Aktualisierungen Ihre dauerhaften Anmeldeinformationen besorgen und installieren (siehe *Anfordern und Hinzufügen von Anmeldeinformationen für Regelaktualisierungen*).

Wenn Sie Common Criteria- und FIPS-Vorschriften einhalten müssen, sollten Sie ESM nicht auf diese Weise aktualisieren. Zertifizierte Aktualisierungen erhalten Sie vom McAfee-Support.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .
2. Klicken Sie auf die Geräteoption **Verwaltung | Gerät aktualisieren**.
3. Wählen Sie in der Tabelle eine Aktualisierung aus, oder klicken Sie auf **Durchsuchen**, um die Aktualisierung auf dem lokalen System zu suchen.

Das Gerät wird mit der aktualisierten Softwareversion neu gestartet.

Anordnen der Geräte

In der Systemnavigationsstruktur werden die im System vorhandenen Geräte aufgeführt. Mit der Funktion Anzeigetyp können Sie auswählen, wie die Geräte angezeigt werden sollen.

Wenn mehr Geräte zum System hinzukommen, ist eine logische Anordnung sinnvoll, damit Sie die jeweils benötigten Geräte leichter finden können. Wenn Sie beispielsweise Büros an verschiedenen Standorten haben, bietet es sich möglicherweise an, die jeweilige Zone anzuzeigen.

Sie können drei vordefinierte Anzeigen verwenden und benutzerdefinierte Anzeigen entwerfen. Innerhalb jeder benutzerdefinierten Anzeige können Sie Gruppen hinzufügen, um die Anordnung der Geräte weiter zu untergliedern.

Einrichten der Steuerung des Netzwerkverkehrs auf einem Gerät

Definieren Sie einen Höchstwert für die Datenausgabe für Empfängergeräte sowie für ACE-, ELM-, Nitro IPS-, ADM- und DEM-Geräte.

Diese Funktion ist hilfreich, wenn Einschränkungen für die Bandbreite gelten und Sie die Menge der Daten steuern möchten, die von den einzelnen Geräten gesendet werden können. Dabei können Sie zwischen Kilobit (KBit), Megabit (MBit) und Gigabit (GBit) pro Sekunde wählen.

Seien Sie vorsichtig, wenn Sie diese Funktion konfigurieren, da es durch Begrenzen des Datenverkehrs zu Datenverlusten kommen kann.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf die Option **Konfiguration** für das Gerät, auf **Schnittstellen** und dann auf die Registerkarte **Datenverkehr**.

Die vorhandenen Steuerungen werden in der Tabelle aufgeführt.

3 Zum Hinzufügen von Steuerungen für ein Gerät klicken Sie auf **Hinzufügen**, geben Sie die Netzwerkadresse und die Maske ein, legen Sie die Rate fest, und klicken Sie dann auf **OK**.

Wenn Sie die Maske auf Null (0) festlegen, werden alle gesendeten Daten gesteuert.

4 Klicken Sie auf **Anwenden**.

Die Geschwindigkeit des ausgehenden Datenverkehrs wird für die angegebene Netzwerkadresse gesteuert.

Gerätekonfiguration

Die Seite **Konfiguration** für jedes Gerät enthält Optionen zum Konfigurieren von Einstellungen wie beispielsweise Netzwerkschnittstelle, SNMP-Benachrichtigungen, NTP-Einstellungen und ELM-Protokollierung.

Einrichten von Netzwerkschnittstellen

Mit Schnittstelleneinstellungen bestimmen Sie, wie die Verbindung zwischen ESM und dem Gerät hergestellt wird. Sie müssen diese Einstellungen für jedes Gerät definieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie für das Gerät auf die Option **Konfiguration** und dann auf **Schnittstellen**.

3 Geben Sie die erforderlichen Daten ein, und klicken Sie dann auf **Anwenden**.

Alle Änderungen werden mithilfe von Push an das Gerät übertragen und werden sofort wirksam. Beim Anwenden der Änderungen wird das Gerät erneut initialisiert, wodurch alle aktuellen Sitzungen getrennt werden.

Verwalten von Netzwerkschnittstellen

Die Kommunikation mit einem Gerät kann über die öffentlichen und privaten Schnittstellen der Datenverkehrspfade erfolgen. Dies bedeutet, dass das Gerät im Netzwerk nicht sichtbar ist, da es keine IP-Adresse benötigt.

Verwaltungsschnittstelle

Netzwerkadministratoren können alternativ eine Verwaltungsschnittstelle mit einer IP-Adresse für die Kommunikation zwischen ESM und dem Gerät konfigurieren. Für die folgenden Funktionen eines Geräts muss eine Verwaltungsschnittstelle verwendet werden:

- Vollständige Kontrolle über Umgehungs-Netzwerkkarten
- Verwenden der Zeitsynchronisierung über NTP
- Vom Geräten generiertes Syslog
- SNMP-Benachrichtigungen

Geräte sind mit mindestens einer Verwaltungsschnittstelle ausgestattet, über die das Gerät eine IP-Adresse erhält. Mit einer IP-Adresse ist der direkte Zugriff auf das Gerät durch ESM möglich, ohne dass die Kommunikation an eine andere Ziel-IP-Adresse oder einen anderen Hostnamen geleitet werden muss.



Verbinden Sie die Verwaltungsschnittstelle des Netzwerks nicht mit einem öffentlichen Netzwerk, da sie dann für das öffentliche Netzwerk sichtbar ist und ihre Sicherheit kompromittiert werden kann.

Bei einem Gerät im Nitro IPS-Modus benötigen Sie für jeden Pfad des Netzwerkverkehrs zwei Schnittstellen. Für den IDS-Modus sind mindestens zwei Netzwerkschnittstellen im Gerät erforderlich. Sie können im Gerät mehrere Verwaltungsschnittstellen für das Netzwerk konfigurieren.

Umgehungs-Netzwerkkarte

Für ein Gerät im Umgehungsmodus wird sämtlicher Verkehr zugelassen, auch bösartiger Datenverkehr. Unter normalen Umständen kann es ein bis drei Sekunden lang zu einem Verbindungsverlust kommen, wenn das Gerät in den Umgehungsmodus wechselt. Beim Verlassen des Umgehungsmodus kann die Verbindung für 18 Sekunden getrennt werden. Bei Verbindungen mit bestimmten Switches, beispielsweise einigen Modellen von Cisco Catalyst, sind andere Zahlen möglich. In diesem Fall kann die Verbindung 33 Sekunden lang getrennt werden, wenn das Gerät in den Umgehungsmodus wechselt oder diesen verlässt.

In dem Szenario, in dem es 33 Sekunden dauert, die Kommunikation wieder herzustellen, können Sie Portfast für den Switch-Port aktivieren und die Geschwindigkeit sowie den Duplex-Modus manuell festlegen, um wieder normale Zeiten zu erzielen. Achten Sie darauf, für alle vier Ports (Switch, beide Ports von Nitro IPS und den Port des anderen Geräts) die gleiche Einstellung festzulegen. Anderenfalls tritt möglicherweise im Umgehungsmodus ein Aushandlungsproblem auf (siehe *Einrichten von Umgehungs-Netzwerkkarten*).

Die verfügbaren Umgehungsoptionen hängen vom Typ der Umgehungs-Netzwerkkarte im Gerät ab (Typ 2 oder Typ 3).

Hinzufügen von statischen Routen

Bei einer statischen Route handelt es sich um einen Satz von Anweisungen, aus denen hervorgeht, wie Hosts oder Netzwerke erreicht werden können, die nicht über das Standard-Gateway verfügbar sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf **Konfiguration** | **Schnittstellen**.

3 Klicken Sie neben der Tabelle **Statische Routen** auf **Hinzufügen**.

4 Geben Sie die Informationen ein, und klicken Sie dann auf **OK**.

Umgehungs-Netzwerkkarte

Unter normalen Umständen kann es ein bis drei Sekunden lang zu einem Verbindungsverlust kommen, wenn das Gerät in den Umgehungsmodus wechselt. Beim Verlassen des Umgehungsmodus kann die Verbindung für 18 Sekunden getrennt werden. Bei Verbindungen mit bestimmten Switches, beispielsweise einigen Modellen von Cisco Catalyst, sind andere Zahlen möglich. In diesem Fall kann die Verbindung 33 Sekunden lang getrennt werden, wenn das Gerät in den Umgehungsmodus wechselt oder diesen verlässt.

In dem Szenario, in dem es 33 Sekunden dauert, die Kommunikation wieder herzustellen, können Sie Portfast für den Switch-Port aktivieren und die Geschwindigkeit sowie den Duplex-Modus manuell festlegen, um wieder normale Zeiten zu erzielen. Achten Sie darauf, für alle vier Ports (Switch, beide Ports von Nitro IPS und den Port des anderen Geräts) die gleiche Einstellung festzulegen. Anderenfalls tritt möglicherweise im Umgehungsmodus ein Aushandlungsproblem auf.

Die verfügbaren Umgehungsoptionen hängen vom Typ der Umgehungs-Netzwerkkarte im Gerät ab (Typ 2 oder Typ 3).

Einrichten von Umgehungs-Netzwerkkarten

Auf IPS-Geräten können Sie Einstellungen für eine Umgehungs-Netzwerkkarte definieren, um sämtlichen Verkehr passieren zu lassen.

ADM-und DEM-Geräte befinden sich immer im IDS-Modus. Sie können Typ und Status der Umgehungs-Netzwerkkarte anzeigen, aber Sie können die Einstellungen nicht ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf **Konfiguration** | **Schnittstellen**.

3 Wechseln Sie auf der Seite **Einstellungen für Netzwerkschnittstellen** unten zum Abschnitt **Konfiguration für Umgehungs-Netzwerkkarte**.

4 Sie können Typ und Status anzeigen oder auf einem IPS-Gerät die Einstellungen ändern.

5 Klicken Sie auf **OK**.

Hinzufügen von VLANs und Aliassen

Fügen Sie virtuelle lokale Netzwerke (Virtual Local Area Networks, VLANs) und Aliasse (zugewiesene Paare aus IP-Adresse und Netzmaske, die Sie hinzufügen, wenn Sie ein Netzwerkgerät mit mehreren IP-Adressen haben) zu einer ACE- oder ELM-Schnittstelle hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf die Geräteoption **Konfiguration**, auf **Schnittstellen** und dann auf **Erweitert**.
3. Klicken Sie auf **VLAN hinzufügen**, geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.
4. Wählen Sie das VLAN aus, zu dem Sie den Alias hinzufügen möchten, und klicken Sie dann auf **Alias hinzufügen**.
5. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Konfigurieren von SNMP-Benachrichtigungen

Zum Konfigurieren der von Geräten generierten SNMP-Benachrichtigungen müssen Sie festlegen, welche Traps gesendet werden sollen, und die Ziele für die Traps angeben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Konfiguration** | **SNMP**.
3. Definieren Sie die Einstellungen, und klicken Sie dann auf **OK**.

Einrichten von NTP auf einem Gerät

Synchronisieren Sie die Gerätezeit über einen NTP-Server (Network Time Protocol) mit ESM.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Konfiguration** | **NTP**.
3. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Aufgaben

- *Anzeigen des Status von NTP-Servern* auf Seite 180
  Zeigen Sie den Status aller NTP-Server auf dem ESM-Gerät an.

Synchronisieren des Geräts mit ESM

Wenn Sie das ESM-Gerät ersetzen müssen, importieren Sie die Schlüssel der einzelnen Geräte, damit Sie die Einstellungen wiederherstellen können. Wenn keine aktuelle Datenbanksicherung vorhanden ist, müssen Sie außerdem die Einstellungen für Datenquellen, virtuelle Geräte und Datenbank-Server mit ESM synchronisieren, damit der Abruf von Ereignissen fortgesetzt wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf **Konfiguration** | **Gerät synchronisieren**.

3 Klicken Sie nach Abschluss der Synchronisierung auf **OK**.

Einrichten der Kommunikation mit ELM

Wenn Sie die Daten von diesem Gerät an das ELM-Gerät senden, werden auf der Seite **Konfiguration** des Geräts die Optionen **ELM-IP** und **ELM synchronisieren** angezeigt. Mit diesen Optionen können Sie die IP-Adresse aktualisieren und das ELM-Gerät mit dem Gerät synchronisieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf **Konfiguration**, und führen Sie dann einen der folgenden Schritte aus:

Option	Aufgabe
ELM-IP	Aktualisieren Sie die IP-Adresse für das ELM-Gerät, mit dem dieses Gerät verknüpft ist. So müssen Sie vorgehen, wenn Sie die IP-Adresse für das ELM-Gerät ändern oder die ELM-Verwaltungsschnittstelle ändern, über die dieses Gerät mit dem ELM-Gerät kommuniziert.
ELM synchronisieren	Synchronisieren Sie das ELM-Gerät mit dem Gerät, wenn eines der beiden Geräte ersetzt wurde. Wenn Sie diese Funktion verwenden, wird die SSH-Kommunikation zwischen den beiden Geräten wieder hergestellt. Dabei wird der Schlüssel für das neue Gerät mit den vorherigen Einstellungen verwendet.

Festlegen des standardmäßigen Protokollierungspools

Wenn im System ein ELM-Gerät vorhanden ist, können Sie ein Gerät so einrichten, dass die von diesem Gerät empfangenen Ereignisdaten an das ELM-Gerät gesendet werden. Dazu müssen Sie den standardmäßigen Protokollierungspool konfigurieren.

Ereignisse werden erst an das ELM-Gerät gesendet, wenn der Zeitraum für die Aggregation abgelaufen ist.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf **Konfiguration** | **Protokollierung**.

3 Wählen Sie auf den daraufhin geöffneten Seiten die entsprechenden Optionen aus.

Wenn die Protokollierung der Daten von diesem Gerät auf dem ELM-Gerät aktiviert ist, werden Sie informiert.

Allgemeine Geräteinformationen und -einstellungen

Für jedes Gerät gibt es eine Seite mit allgemeinen Informationen zum Gerät, beispielsweise Seriennummer und Softwareversion. Außerdem können Sie Einstellungen für das Gerät definieren. Beispielsweise können Sie die Zone auswählen und die Uhr synchronisieren.

Anzeigen von Nachrichtenprotokollen und Gerätestatistiken

Sie können vom System generierte Nachrichten oder Statistiken zur Leistung des Geräts anzeigen oder eine TGZ-Datei mit Informationen zum Gerätestatus herunterladen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf die Geräteoption **Verwaltung**, und wählen Sie dann eine der folgenden Optionen aus:

Option	Beschreibung
Protokoll anzeigen	Klicken Sie auf diese Option, um vom System aufgezeichnete Nachrichten anzuzeigen. Klicken Sie auf **Gesamte Datei herunterladen**, um die Daten in eine Datei herunterzuladen.
Statistik anzeigen	Klicken Sie auf diese Option, um Statistiken zur Leistung des Geräts anzuzeigen, beispielsweise zur Ethernet-Schnittstelle und zu den Filtern ifconfig und iptables.
Gerätedaten	Klicken Sie auf diese Option, um eine TGZ-Datei mit Daten zum Status des Geräts herunterzuladen. Diese Option können Sie verwenden, wenn Sie gemeinsam mit dem McAfee-Support ein Problem auf dem System beheben.

Aktualisieren der Software eines Geräts

Wenn die Software auf einem Gerät veraltet ist, laden Sie aus einer Datei auf dem ESM-Gerät oder vom lokalen Computer eine neue Version der Software hoch.

Bevor Sie beginnen

Wenn Sie das System seit mehr als 30 Tagen besitzen, müssen Sie sich für den Zugriff auf die Aktualisierungen Ihre dauerhaften Anmeldeinformationen besorgen und installieren (siehe *Anfordern und Hinzufügen von Anmeldeinformationen für Regelaktualisierungen*).



Wenn Sie Common Criteria- und FIPS-Vorschriften einhalten müssen, sollten Sie ESM nicht auf diese Weise aktualisieren. Zertifizierte Aktualisierungen erhalten Sie vom McAfee-Support.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf die Geräteoption **Verwaltung | Gerät aktualisieren**.

3 Wählen Sie in der Tabelle eine Aktualisierung aus, oder klicken Sie auf **Durchsuchen**, um die Aktualisierung auf dem lokalen System zu suchen.

Das Gerät wird mit der aktualisierten Softwareversion neu gestartet.

Eingeben von Linux-Befehlen für ein Gerät

Mit der Option **Terminal** können Sie Linux-Befehle auf einem Gerät eingeben. Diese Funktion ist für fortgeschrittene Benutzer gedacht und darf nur in Notfällen unter Anleitung von Mitarbeitern des McAfee-Supports verwendet werden.

Diese Option ist nicht FIPS-konform und ist im FIPS-Modus deaktiviert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf die Geräteoption **Verwaltung** | **Terminal**.
3. Geben Sie das Systemkennwort ein, und klicken Sie dann auf **OK**.
4. Geben Sie die Linux-Befehle ein, exportieren Sie die Datei, oder übertragen Sie Dateien.
5. Klicken Sie auf **Schließen**.

Gewähren des Zugriffs auf das System

Wenn Sie sich an den Support von McAfee wenden, müssen Sie möglicherweise den Zugriff auf Ihr System gewähren, damit der Mitarbeiter des technischen Supports Einblick in das System nehmen kann.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf die Geräteoption **Verwaltung** | **Verbinden**.

   Die Schaltfläche ändert sich in **Trennen**, und Ihre IP-Adresse wird angezeigt.
3. Geben Sie dem Mitarbeiter des technischen Supports die IP-Adresse.

   Möglicherweise müssen Sie weitere Informationen angeben, beispielsweise das Kennwort.
4. Klicken Sie auf **Trennen**, um die Verbindung zu beenden.

Überwachen des Datenverkehrs

Wenn Sie den durch ein DEM-, ADM- oder IPS-Gerät fließenden Datenverkehr überwachen müssen, können Sie mit **TCP-Abbild sichern** eine Instanz des auf dem Gerät ausgeführten Linux-Programms herunterladen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf die Geräteoption **Verwaltung**.
3. Führen Sie auf dieser Seite im Abschnitt **TCP-Abbild sichern** die Schritte zum Herunterladen der Instanz aus.

Anzeigen von Geräteinformationen

Zeigen Sie allgemeine Informationen zu einem Gerät an. Öffnen Sie die Seite **Informationen** für das Gerät, um unter anderem System-ID, Seriennummer, Modell, Version und Build anzuzeigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Zeigen Sie die verfügbaren Informationen an, und klicken Sie dann auf **OK**.

Starten, Anhalten, Neustarten oder Aktualisieren eines Geräts

Auf der Seite **Informationen** können Sie ein Gerät starten, anhalten, neu starten oder aktualisieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Vergewissern Sie sich, dass **Geräteinformationen** ausgewählt ist, und klicken Sie dann auf **Starten**, **Anhalten**, **Neu starten** oder **Aktualisieren**.

Ändern des Gerätenamens

Beim Hinzufügen eines Geräts zur Systemstruktur geben Sie dem Gerät einen Namen, der in der Struktur angezeigt wird. Diesen Namen, den Systemnamen, die URL und die Beschreibung können Sie ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Name und Beschreibung**, ändern Sie dann den Namen, den Systemnamen, die URL und die Beschreibung, oder zeigen Sie die **Geräte-ID** an.
3. Klicken Sie auf **OK**.

Hinzufügen eines URL-Links

Zum Anzeigen von Geräteinformationen über eine URL können Sie den Link für jedes Gerät auf der Seite **Name und Beschreibung** einrichten. Auf den hinzugefügten Link können Sie in den Ansichten **Ereignisanalyse** und **Flussanalyse** für jedes Gerät zugreifen, indem Sie unten in den Ansichtskomponenten auf das Symbol **URL zum Starten des Geräts**  klicken.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Name und Beschreibung**, und geben Sie dann die URL ein.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Ändern der Verbindung mit ESM

Wenn Sie ein Gerät zu ESM hinzufügen, richten Sie die Verbindung des Geräts mit ESM ein. Sie können die IP-Adresse und den Port ändern, die SSH-Kommunikation deaktivieren und den Status der Verbindung überprüfen.



Wenn Sie diese Einstellungen ändern, hat dies keine Auswirkungen auf das Gerät selbst. Die Änderungen wirken sich nur auf die Kommunikation zwischen ESM und dem Gerät aus.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Verbindung**, und nehmen Sie dann die Änderungen vor.
3. Klicken Sie auf **Anwenden**.

Ereignisse, Flüsse und Protokolle

Auf IPS-Geräten, ADM-Geräten und Empfängergeräten werden Ereignisse, Flüsse und Protokolle erfasst, auf ACE- und DEM-Geräten Ereignisse und Protokolle und auf ELM-Geräten Protokolle. Legen Sie für die einzelnen Geräte fest, dass diese Elemente manuell oder automatisch überprüft werden sollen. Außerdem können Sie die von einem Gerät generierten Ereignisse oder Flüsse aggregieren.

Einrichten von Downloads für Ereignisse, Flüsse und Protokolle

Überprüfen Sie manuell, ob Ereignisse, Flüsse und Protokolle vorhanden sind, oder legen Sie fest, dass diese Überprüfung automatisch vom Gerät ausgeführt wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Ereignisse, Flüsse und Protokolle**, **Ereignisse und Protokolle** oder **Protokolle**.
3. Richten Sie die Downloads ein, und klicken Sie dann auf **Anwenden**.

Definieren von Geolocation- und ASN-Einstellungen

Über *Geolocation* erhalten Sie den tatsächlichen geografischen Standort von mit dem Internet verbundenen Computern. *ASN (Autonomous System Number)* ist eine Zahl, die einem autonomen System zugewiesen wird und jedes Netzwerk im Internet eindeutig identifiziert.

Mithilfe dieser beiden Datentypen können Sie den physischen Standort einer Bedrohung identifizieren. Daten für Quell- und Ziel-Geolocation können für Ereignisse erfasst werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf **Ereignisse, Flüsse und Protokolle** oder **Ereignisse und Protokolle** und dann auf **Geolocation**.

3 Wählen Sie die entsprechenden Optionen zum Generieren der gewünschten Informationen aus, und klicken Sie dann auf **OK**.

Anhand dieser Informationen können Sie Ereignisdaten filtern.

Aggregieren von Ereignissen oder Flüssen

Ein Ereignis oder Fluss kann theoretisch tausendfach generiert werden. Sie müssen nicht Tausende identischer Ereignisse durchgehen, sondern können mithilfe der Aggregation diese Ereignisse als ein einziges Ereignis bzw. einen einzigen Fluss anzeigen. Dabei gibt ein Zähler an, wie oft ein Ereignis aufgetreten ist.

Bei der Aggregation wird der Speicherplatz sowohl auf dem Gerät als auch in ESM effizienter genutzt, da nicht jedes einzelne Paket gespeichert werden muss. Diese Funktion gilt nur für Regeln, für die im **Richtlinien-Editor** die Aggregation aktiviert ist.

Quell-IP-Adresse und Ziel-IP-Adresse

Die "nicht festgelegten" Werte oder aggregierten Werte für Quell-IP-Adresse und Ziel-IP-Adresse werden in allen Ergebnissätzen als "::" anstelle von "0.0.0.0" angezeigt. Beispiel:

- `::ffff:10.0.12.7` wird als `0:0:0:0:0:FFFF:A00:C07` eingefügt (`A00:C07` entspricht `10.0.12.7`).
- `::0000:10.0.12.7` entspricht `10.0.12.7`.

Aggregierte Ereignisse und Flüsse

In aggregierten Ereignissen und Flüssen wird mit den Feldern Erstes Mal, Letztes Mal und Insgesamt die Dauer und Menge der Aggregation angegeben. Beispiel: Ein Ereignis ist in den ersten zehn Minuten nach 12:00 Uhr 30 Mal aufgetreten. Das Feld **Erstes Mal** enthält die Uhrzeit 12:00 Uhr (den Zeitpunkt der ersten Instanz des Ereignisses), das Feld **Letztes Mal** enthält die Uhrzeit 12:10 Uhr (den Zeitpunkt der letzten Instanz des Ereignisses), und das Feld **Insgesamt** enthält den Wert 30.

Sie können die Standardeinstellungen für Ereignisse oder die Flussaggregation für das Gerät insgesamt ändern und für einzelne Regeln Ausnahmen für die Einstellungen des Geräts hinzufügen (siehe *Verwalten von Aggregationsausnahmen für Ereignisse*).

Die dynamische Aggregation ist auch standardmäßig aktiviert. Wenn sie ausgewählt ist, werden die Einstellungen für **Aggregationsebene 1** ersetzt und die Einstellungen für **Aggregationsebene 2** und **Aggregationsebene 3** erhöht. Datensätze werden basierend auf der Abrufeinstellung für Ereignisse, Flüsse und Protokolle abgerufen. Wenn automatisches Abrufen festgelegt ist, wird ein Datensatz nur beim ersten Abruf durch ESM vom Gerät komprimiert. Wenn manuelles Abrufen festgelegt ist, wird ein Datensatz bis zu 24 Stunden lang komprimiert oder bis zum manuellen Abruf eines neuen Datensatzes, je nachdem, was zuerst geschieht. Wenn das 24-Stunden-Limit für die Komprimierung erreicht ist, wird ein neuer Datensatz abgerufen, und die Komprimierung beginnt für diesen neuen Datensatz.

Ändern von Einstellungen für die Ereignis- oder Flussaggregation

Ereignisaggregation und Flussaggregation sind standardmäßig aktiviert und auf **Hoch** festgelegt. Sie können die Einstellungen nach Bedarf ändern. Die Auswirkungen der einzelnen Einstellungen werden auf der Seite **Aggregation** beschrieben.

Bevor Sie beginnen

Zum Ändern dieser Einstellungen benötigen Sie die Berechtigungen **Richtlinienadministrator** und **Geräteverwaltung** oder **Richtlinienadministrator** und **Benutzerdefinierte Regeln**.

Die Ereignisaggregation ist nur für ADM- und IPS-Geräte sowie Empfängergeräte verfügbar, die Flussaggregation ist für IPS-Geräte und Empfängergeräte verfügbar.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Ereignisaggregation** oder **Flussaggregation**.

3 Definieren Sie die Einstellungen, und klicken Sie dann auf **OK**.

Verwalten von Aggregationsausnahmen für Ereignisse

Sie können eine Liste der Aggregationsausnahmen für Ereignisse anzeigen, die zum System hinzugefügt wurden. Außerdem können Sie eine Ausnahme bearbeiten oder entfernen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Ereignisaggregation** und dann unten auf dem Bildschirm auf **Ansicht**.

3 Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf **Schließen**.

Hinzufügen von Ausnahmen für Einstellungen für die Ereignisaggregation

Aggregationseinstellungen gelten für alle von einem Gerät generierten Ereignisse. Sie können Ausnahmen für einzelne Regeln erstellen, wenn die allgemeinen Einstellungen für die von der jeweiligen Regel generierten Ereignisse nicht gelten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im Ansichtsbereich ein Ereignis aus, das von der Regel generiert wurde, für die Sie eine Ausnahme hinzufügen möchten.

2 Klicken Sie auf das Symbol **Menü**  , und wählen Sie dann **Aggregationseinstellungen ändern** aus.

3 Wählen Sie in den Dropdown-Listen **Feld 2** und **Feld 3** die zu aggregierenden Feldtypen aus.

Sie müssen in **Feld 2** und **Feld 3** unterschiedliche Typen auswählen, da ansonsten ein Fehler auftritt. Wenn Sie diese Feldtypen auswählen, werden die Beschreibungen der einzelnen Aggregationsebenen geändert und spiegeln nun die ausgewählten Optionen wider. Die Zeitlimits für die einzelnen Ebenen hängen von der für das Gerät definierten Einstellung für die Ereignisaggregation ab.

4 Klicken Sie auf **OK**, um die Einstellungen zu speichern und dann auf **Ja**, um fortzufahren.

5 Heben Sie die Auswahl von Geräten auf, für die Sie keinen Rollout der Änderungen ausführen möchten.

6 Klicken Sie auf **OK**, um den Rollout für die Änderungen auf den ausgewählten Geräten auszuführen.

In der Spalte **Status** wird beim Rollout der Änderungen der Aktualisierungsstatus angezeigt.

Virtuelle Geräte

Sie können zu einigen Nitro IPS- und ADM-Gerätemodellen virtuelle Geräte hinzufügen, um den Datenverkehr zu überwachen, Datenverkehrsmuster zu vergleichen und Berichte zu erstellen.

Zweck und Vorteile

Virtuelle Geräte können für verschiedene Zwecke verwendet werden:

- Sie können Datenverkehrsmuster mit Regelsätzen vergleichen. Beispielsweise können Sie, um Web-Datenverkehr mit Web-Regeln zu vergleichen, ein virtuelles Gerät einrichten, von dem nur Ports für Web-Datenverkehr untersucht werden, und eine Richtlinie einrichten, mit der Sie verschiedene Regeln aktivieren oder deaktivieren können.
- Sie können Berichte erstellen. Wenn Sie virtuelle Geräte auf diese Weise verwenden, ist dies mit einer automatischen Filterung vergleichbar.
- Sie können mehrere Verkehrspfade gleichzeitig überwachen. Wenn Sie ein virtuelles Gerät verwenden, können Sie für jeden Verkehrspfad eigene Richtlinien festlegen und verschiedene Verkehrsarten nach unterschiedlichen Richtlinien sortieren.

Maximale Anzahl der Geräte pro Modell

Wie viele virtuelle Geräte zu einem ADM-Gerät oder Nitro IPS-Gerät hinzugefügt werden können, hängt vom Modell ab:

Maximale Anzahl der Geräte	Modell
2	APM-1225 NTP-1225 APM-1250 NTP-1250
4	APM-2230 NTP-2230 NTP-2600 APM-3450 NTP-3450

Maximale Anzahl der Geräte	Modell
8	NTP-2250 NTP-4245 NTP-5400
0	APM-VM NTP-VM

Verwendung von Auswahlregeln

Auswahlregeln werden als Filter verwendet, mit denen Sie festlegen können, welche Pakete von einem virtuellen Gerät verarbeitet werden.

Damit ein Paket mit einer Auswahlregel übereinstimmt, müssen alle in der Regel definierten Filterkriterien erfüllt sein. Wenn die Informationen des Pakets mit allen Filterkriterien für eine einzige Auswahlregel übereinstimmen, wird das Paket von dem virtuellen Gerät verarbeitet, das die übereinstimmende Auswahlregel enthält. Anderenfalls wird das Paket an das nächste virtuelle Gerät in der Reihenfolge weitergegeben dann standardmäßig vom ADM- oder Nitro IPS-Gerät selbst verarbeitet, wenn auf keinem virtuellen Gerät übereinstimmende Auswahlregeln vorhanden sind.

Beachten Sie bei virtuellen IPv4-Geräten Folgendes:

- Alle Pakete für eine einzige Verbindung werden ausschließlich basierend auf dem ersten Paket in der Verbindung sortiert. Wenn das erste Paket in einer Verbindung mit einer Auswahlregel für das dritte virtuelle Gerät in der Liste übereinstimmt, werden alle nachfolgenden Pakete in dieser Verbindung an das dritte virtuelle Gerät weitergeleitet. Dies ist auch dann der Fall, wenn die Pakete mit einem virtuellen Gerät übereinstimmen, das sich in der Liste an einer höheren Position befindet.
- Ungültige Pakete (Pakete, durch die nicht eine Verbindung eingerichtet wird oder die nicht Bestandteil einer hergestellten Verbindung sind) werden auf dem Basisgerät einsortiert. Beispiel: Sie verwenden ein virtuelles ADM-Gerät, auf dem nach Paketen mit dem Quell- oder Ziel-Port 80 gesucht wird. Wenn ein ungültiges Paket mit dem Quell- oder Ziel-Port 80 durchgeleitet wird, geschieht Folgendes: Das Paket wird nicht an das virtuelle Gerät weitergeleitet, das nach Datenverkehr an Port 80 sucht, sondern auf dem Basisgerät einsortiert. Daher sehen Sie auf dem Basisgerät Ereignisse, die so aussehen, als hätten sie an ein virtuelles Gerät weitergeleitet werden sollen.

Die Reihenfolge der Auswahlregeln ist wichtig, da das erste Paket, das mit einer Regel übereinstimmt, automatisch zur Verarbeitung an das entsprechende virtuelle Gerät weitergeleitet wird. Beispiel: Sie fügen vier Auswahlregeln hinzu, und die vierte Regel ist der Filter, der am häufigsten ausgelöst wird. Dies bedeutet, dass die anderen Filter für dieses virtuelle Gerät von jedem Paket passiert werden müssen, bevor die am häufigsten ausgelöste Auswahlregel erreicht ist. Um die Verarbeitung effizienter zu gestalten, führen Sie den am häufigsten ausgelösten Filter nicht an letzter, sondern an erster Stelle auf.

Reihenfolge der virtuellen Geräte

Die Reihenfolge der Überprüfung der virtuellen Geräte ist wichtig, da die beim ADM- oder Nitro IPS-Gerät eingehenden Pakete in der Reihenfolge mit den Auswahlregeln für jedes virtuelle Gerät verglichen werden, in der die virtuellen Geräte eingerichtet wurden. Das Paket erreicht die Auswahlregeln für das zweite virtuelle Gerät nur, wenn es keiner Auswahlregel auf dem ersten Gerät entspricht.

- Die Reihenfolge auf einem ADM-Gerät können Sie auf der Seite **Virtuelles Gerät bearbeiten** ändern (**ADM-Eigenschaften** | **Virtuelle Geräte** | **Bearbeiten**). Bringen Sie die Filter mithilfe der Pfeile in die richtige Reihenfolge.
- Die Reihenfolge auf einem Nitro IPS-Gerät können Sie mit den Pfeilen auf der Seite **Virtuelle Geräte** ändern (**IPS-Eigenschaften** | **Virtuelle Geräte**).

Virtuelle ADM-Geräte

Mit virtuellen ADM-Geräten überwachen Sie den Datenverkehr an einer Schnittstelle. Es sind bis zu vier ADM-Schnittstellenfilter im System möglich. Jeder Filter kann nur auf jeweils ein virtuelles ADM-Gerät angewendet werden. Wenn ein Filter einem virtuellen ADM-Gerät zugewiesen ist, wird er erst in der Liste der verfügbaren Filter angezeigt, wenn er von dem jeweiligen Gerät entfernt wurde.

Ungültige Pakete (Pakete, durch die nicht eine Verbindung eingerichtet wird oder die nicht Bestandteil einer hergestellten Verbindung sind) werden auf dem Basisgerät einsortiert. Wenn Sie beispielsweise ein virtuelles ADM-Gerät verwenden, auf dem nach Paketen mit dem Quell- oder Ziel-Port 80 gesucht wird, und ein ungültiges Paket mit dem Quell- oder Ziel-Port 80 durchgeleitet wird, geschieht Folgendes: Das Paket wird nicht an das virtuelle ADM-Gerät weitergeleitet, das nach Datenverkehr an Port 80 sucht, sondern auf dem Basisgerät einsortiert. Daher sehen Sie möglicherweise auf dem Basisgerät Ereignisse, die so aussehen, als hätten sie an ein virtuelles ADM-Gerät weitergeleitet werden sollen.

Verwalten von Auswahlregeln

Auswahlregeln werden als Filter verwendet, mit denen Sie festlegen können, welche Pakete von einem virtuellen Gerät verarbeitet werden. Sie können Auswahlregeln hinzufügen, bearbeiten und löschen.

Die Reihenfolge der Auswahlregeln ist wichtig, da das erste Paket, das mit einer Regel übereinstimmt, automatisch zur Verarbeitung an das entsprechende virtuelle Gerät weitergeleitet wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie einen IPS- oder ADM-Geräteknoten aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Virtuelle Geräte**und dann auf **Hinzufügen**.

Das Fenster **Virtuelles Gerät hinzufügen** wird geöffnet.

3 Sie können in der Tabelle Auswahlregeln hinzufügen, bearbeiten, entfernen oder ihre Reihenfolge ändern.

Hinzufügen eines virtuellen Geräts

Sie können auf einigen ADM- und IPS-Geräten ein virtuelles Gerät hinzufügen und durch Festlegen von Auswahlregeln bestimmen, welche Pakete von den einzelnen Geräten verarbeitet werden.

Bevor Sie beginnen

Vergewissern Sie sich, dass zum ausgewählten Gerät virtuelle Geräte hinzugefügt werden können (siehe *Informationen zu virtuellen Geräten*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein ADM- oder IPS-Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf **Virtuelle Geräte** | **Hinzufügen**.

3 Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

4 Klicken Sie auf **Schreiben**, um die Einstellungen zum Gerät hinzuzufügen.

Verwalten benutzerdefinierter Anzeigetypen

Sie können die Anordnung der Geräte in der Systemnavigationsstruktur definieren, indem Sie benutzerdefinierte Anzeigetypen hinzufügen, bearbeiten oder löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Systemnavigationsbereich auf den Dropdown-Pfeil für den Anzeigetyp.

2 Führen Sie einen der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Hinzufügen eines benutzerdefinierten Anzeigetyps	1 Klicken Sie auf **Anzeige hinzufügen**. 2 Füllen Sie die Felder aus, und klicken Sie dann auf **OK**.
Bearbeiten eines benutzerdefinierten Anzeigetyps	1 Klicken Sie neben dem zu bearbeitenden Anzeigetyp auf das Symbol **Bearbeiten** . 2 Nehmen Sie Änderungen an den Einstellungen vor, und klicken Sie dann auf **OK**.
Löschen eines benutzerdefinierten Anzeigetyps	Klicken Sie neben dem zu löschenden Anzeigetyp auf das Symbol **Löschen** .

Auswählen eines Anzeigetyps

Wählen Sie aus, wie die Geräte in der Systemnavigationsstruktur angezeigt werden sollen.

> **Bevor Sie beginnen**
>
> Zum Auswählen einer benutzerdefinierten Anzeige müssen Sie diese zuerst zum System hinzufügen (siehe *Verwalten benutzerdefinierter Anzeigetypen*).

Vorgehensweise

1 Klicken Sie im Systemnavigationsbereich auf den Dropdown-Pfeil im Feld für den Anzeigetyp.

2 Wählen Sie einen der Anzeigetypen aus.

Die Anordnung der Geräte in der Navigationsstruktur wird geändert und entspricht nun dem Typ, den Sie für die aktuelle Arbeitssitzung ausgewählt haben.

Verwalten einer Gruppe in einem benutzerdefinierten Anzeigetyp

Sie können Gruppen in einem benutzerdefinierten Anzeigetyp verwenden, um Geräte in logischen Gruppierungen anzuordnen.

Bevor Sie beginnen

Fügen Sie einen benutzerdefinierten Anzeigetyp hinzu (siehe *Verwalten benutzerdefinierter Anzeigetypen*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Systemnavigationsbereich auf die Dropdown-Liste für den Anzeigetyp.

2 Wählen Sie die benutzerdefinierte Anzeige aus, und führen Sie dann einen der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Hinzufügen einer neuen Gruppe	1 Klicken Sie auf einen System- oder Gruppenknoten und dann auf der Aktionssymbolleiste auf das Symbol **Gruppe hinzufügen**. 2 Füllen Sie die Felder aus, und klicken Sie dann auf **OK**. 3 Ziehen Sie Geräte in der Anzeige an die gewünschte Stelle, und legen Sie sie ab, um sie zur Gruppe hinzuzufügen. Wenn das Gerät Teil einer Struktur in der Anzeige ist, wird ein doppelter Geräteknoten erstellt. Das Duplikat in der Systemstruktur können Sie anschließend löschen.
Bearbeiten einer Gruppe	Wählen Sie die Gruppe aus, klicken Sie auf das Symbol **Eigenschaften**, und nehmen Sie dann auf der Seite **Gruppeneigenschaften** Änderungen vor.
Löschen einer Gruppe	Wählen Sie die Gruppe aus, und klicken Sie dann auf das Symbol **Gruppe löschen**. Die Gruppe und die darin enthaltenen Geräte werden aus der benutzerdefinierten Anzeige gelöscht. Die Geräte werden nicht aus dem System gelöscht.

Siehe auch

Verwalten benutzerdefinierter Anzeigetypen auf Seite 26

Löschen doppelter Geräte in der Systemnavigationsstruktur

Doppelte Geräteknoten werden in der Systemnavigationsstruktur angezeigt, wenn Sie Geräte aus einer Systemstruktur in eine Gruppe ziehen und dort ablegen oder wenn Gruppen eingerichtet sind und Sie dann ein Upgrade der ESM-Software durchführen. Es wird empfohlen, die doppelten Geräteknoten zu löschen, um Verwirrung zu vermeiden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Systemnavigationsbereich auf die Dropdown-Liste für den Anzeigetyp.

2 Wählen Sie das Symbol **Bearbeiten** neben der Anzeige mit den doppelten Geräten aus.

3 Heben Sie die Auswahl der doppelten Geräte auf, und klicken Sie dann auf **OK**.

Die Geräte, für die Duplikate vorhanden waren, werden jetzt nur in den zugewiesenen Gruppen aufgeführt.

Verwalten mehrerer Geräte

Mit die Option **Verwaltung mehrerer Geräte** können Sie mehrere Geräte gleichzeitig starten, anhalten und neu starten oder die Software auf den Geräten aktualisieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die zu verwaltenden Geräte aus.
2. Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Verwaltung mehrerer Geräte**  .
3. Wählen Sie den auszuführenden Vorgang aus sowie die Geräte, auf denen Sie den Vorgang ausführen möchten, und klicken Sie dann auf **Starten**.

Verwalten von URL-Links für alle Geräte

Sie können für jedes Gerät einen Link einrichten, damit Geräteinformationen über eine URL angezeigt werden können.

Bevor Sie beginnen

Richten Sie die URL-Site für das Gerät ein.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Benutzerdefinierte Einstellungen** | **Geräte-Links**.
2. Zum Hinzufügen oder Bearbeiten einer URL heben Sie das Gerät hervor, klicken Sie auf **Bearbeiten**, und geben Sie dann die URL ein.

   Für das URL-Feld gilt ein Limit von 512 Zeichen.
3. Klicken Sie auf **OK**.

Sie können auf die URL zugreifen, indem Sie für jedes Gerät auf das Symbol **URL zum Starten des Geräts** unten in den Ansichten **Ereignisanalyse** und **Flussanalyse** klicken.

Anzeigen von Zusammenfassungsberichten für Geräte

Aus den Zusammenfassungsberichten für Geräte gehen die Typen und die Anzahl der Geräte in ESM hervor. Außerdem erfahren Sie, wann ein Ereignis von den einzelnen Geräten empfangen wurde. Diese Berichte können im CSV-Format (durch Komma getrennte Werte) exportiert werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Systeminformationen | Berichte anzeigen**.
2. Sie können den Bericht **Anzahl der Gerätetypen** oder **Ereigniszeitpunkt** anzeigen oder exportieren.
3. Klicken Sie auf **OK**.

Anzeigen eines System- oder Geräteprotokolls

System- und Geräteprotokolle enthalten Ereignisse, die auf den Geräten aufgetreten sind. Sie können die Zusammenfassungsseite anzeigen, auf der Sie die Ereignisanzahl und den Zeitpunkt des ersten und letzten Ereignisses in ESM oder auf einem Gerät finden, oder auf der Seite **Systemprotokoll** oder **Geräteprotokoll** eine detaillierte Liste der Ereignisse anzeigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Zeigen Sie eine Zusammenfassung der Ereignisdaten an:
   - Systemdaten: Klicken Sie in **Systemeigenschaften** auf **Systemprotokoll**.
   - Gerätedaten: Klicken Sie auf der Seite **Eigenschaften** für ein Gerät auf **Geräteprotokoll**.
2. Zum Anzeigen des Ereignisprotokolls geben Sie einen Zeitbereich ein, und klicken Sie dann auf **Ansicht**.

Auf der Seite **Systemprotokoll** oder **Geräteprotokoll** werden alle im angegebenen Zeitbereich generierten Ereignisse angezeigt.

Berichte zum Integritätsstatus von Geräten

Neben System-, Gruppen- oder Geräteknoten in der Systemnavigationsstruktur, für die ein Bericht zum Integritätsstatus verfügbar ist, werden Kennzeichnungen  in den folgenden Farben für den Integritätsstatus angezeigt: weiß (Information), gelb (Inaktivität oder Gerätestatus) oder rot

(Kritisch). Wenn Sie auf die Kennzeichnung klicken, werden auf der Seite **Statuswarnungen für Geräte** Optionen zum Anzeigen der Informationen und zum Beheben von Problemen angezeigt.

Kennzeichnung des Knotentyps	Geöffnetes Element
System oder Gruppe	Die Seite **Statuswarnungen für Geräte: Zusammenfassung** stellt eine Zusammenfassung der Statuswarnungen für die Geräte dar, die dem System oder der Gruppe zugeordnet sind. Die folgenden Statuswarnungen können angezeigt werden: • **Partition wurde gelöscht**: Die maximale Größe einer Datenbanktabelle mit Ereignis-, Fluss- oder Protokolldaten wurde erreicht, und es wurde eine Partition gelöscht, um Speicherplatz für neue Datensätze hinzuzufügen. Sie können Ereignis-, Fluss- und Protokolldaten exportieren, um zu verhindern, dass diese dauerhaft verloren sind. • **Speicherplatz**: Eine Festplatte ist voll oder fast voll. Dies kann beispielsweise die Festplatte des ESM-Geräts, des redundanten ESM-Geräts oder eines Remote-Bereitstellungspunkts sein. • **Kritisch**: Das Gerät funktioniert nicht richtig, und der Fehler muss behoben werden. • **Warnung**: Ein Teil des Geräts funktioniert nicht ordnungsgemäß. • **Information**: Das Gerät funktioniert ordnungsgemäß, aber die Ebene des Gerätestatus hat sich geändert. • **Nicht synchronisiert**: Die Einstellungen des ESM-Geräts für virtuelle Geräte, Datenquellen oder Datenbank-Server sind nicht mit den tatsächlichen Einstellungen des Geräts synchronisiert. • **Rollover ausgeführt**: Für die Protokolltabelle des Geräts war nicht mehr genug Speicherplatz verfügbar. Daher wurde ein Rollover ausgeführt. Dies bedeutet, dass die alten Protokolle mit den neuen Protokollen überschrieben werden. • **Inaktiv**: Auf dem Gerät wurden im Zeitraum des Schwellenwerts für Inaktivität keine Ereignisse oder Flüsse generiert. • **Unbekannt**: Es konnte keine Verbindung zwischen ESM und dem Gerät hergestellt werden. Die Kennzeichnungen **Partition wurde gelöscht**, **Speicherplatz**, **Rollover ausgeführt** und **Information** können Sie löschen, indem Sie die Kontrollkästchen neben den Kennzeichnungen aktivieren und auf **Auswahl löschen** oder **Alle löschen** klicken.
Gerät	Die Seite **Statuswarnungen für Geräte** mit Schaltflächen, über die Sie an die entsprechenden Stellen zum Beheben des Problems gelangen. Die Seite kann die folgenden Schaltflächen enthalten: • **Protokoll**: Auf der Seite **Systemprotokoll** (für Lokales ESM-Gerät) oder **Geräteprotokoll** wird eine Zusammenfassung aller Aktionen angezeigt, die für das System oder Gerät ausgeführt wurden. • **Virtuelle Geräte**, **Datenquellen**, **VA-Quellen** oder **Datenbank-Server**: Hier werden die im System vorhandenen Geräte des jeweiligen Typs aufgeführt und können auf Probleme überprüft werden. • **Inaktiv**: Auf der Seite **Schwellenwert für Inaktivität** wird die Schwellenwerteinstellung für alle Geräte angezeigt. Diese Kennzeichnung gibt an, dass im angegebenen Zeitintervall auf dem Gerät kein Ereignis generiert wurde.

Wenn ein Subsystem nach dem Status Warnung oder Kritisch wiederhergestellt wurde, wird die Kennzeichnung Information angezeigt. Nachfolgend werden die einzelnen Typen der Kennzeichnung Information beschrieben.

Status	Beschreibung und Anweisungen
Umgehungsmodus	Der Netzwerkschnittstellen-Controller (Network Interface Controller, NIC) befindet sich im Umgehungsmodus. Dies ist möglicherweise darauf zurückzuführen, dass ein kritischer Systemprozess fehlgeschlagen ist, das Gerät manuell in den Umgehungsmodus versetzt wurde oder ein anderer Fehler aufgetreten ist. Verwenden Sie die folgenden Optionen, um den Umgehungsmodus für das Gerät zu deaktivieren: **Eigenschaften** | **Konfiguration** | **Schnittstellen**.
Deep Packet Inspector wird nicht ausgeführt.	In Deep Packet Inspector (DPI) ist eine Fehlfunktion aufgetreten. Möglicherweise erfolgt die Wiederherstellung ohne Eingriff. Starten Sie anderenfalls das Gerät neu.
Das Firewall-Warnungsprogramm (ngulogd) wird nicht ausgeführt.	In Firewall Alert Aggregator (FAA) ist eine Fehlfunktion aufgetreten. Möglicherweise erfolgt die Wiederherstellung ohne Eingriff. Starten Sie anderenfalls das Gerät neu.
Die Datenbank wird nicht ausgeführt.	Auf dem McAfee Extreme Database-Server (EDB) ist eine Fehlfunktion aufgetreten. Möglicherweise können Sie das Problem durch Neustarten des Geräts beheben. Es kann jedoch sein, dass die Datenbank erneut erstellt werden muss.
Überbelegungsmodus	Wenn das überwachte Netzwerk für Nitro IPS zu stark ausgelastet ist, werden Netzwerkpakete möglicherweise nicht überprüft. Von der Integritätsüberwachung wird eine Warnung generiert, aus der hervorgeht, dass Nitro IPS überbelegt ist. Der Wert für den Überbelegungsmodus ist standardmäßig auf Verwerfen festgelegt. Zum Ändern des Werts navigieren Sie zu **Richtlinien-Editor**, klicken Sie im Bereich **Regeltypen** auf **Variable**, erweitern Sie die Variable **packet_inspection**, und wählen Sie für die Variable **OVERSUBSCRIPTION _MODE** die Option **Vererben** aus. Für diese Variable sind die Werte **passieren lassen** und **Verwerfen** zulässig.
Der Steuerungskanal wird nicht ausgeführt.	Der Prozess für den Kommunikationskanal mit dem ESM-Gerät ist fehlgeschlagen. Möglicherweise kann das Problem durch einen Neustart des Geräts behoben werden.
RDEP oder Syslog-Programme werden nicht ausgeführt.	Bei einer Fehlfunktion des Subsystems für die Behandlung von Drittanbieter-Datenquellen (beispielsweise Syslog oder SNMP) wird die Warnung Kritisch ausgelöst. Eine Warnmeldung der Stufe Warnung wird ausgelöst, wenn die Erfassung in einem bestimmten Zeitraum keine Daten von der Drittanbieter-Datenquelle empfangen hat. Dies ist ein Hinweis darauf, dass die Datenquelle möglicherweise inaktiv ist oder dass nicht wie erwartet Daten an den Empfänger gesendet werden.
Die Kommunikation zwischen der Integritätsüberwachung und dem Controller-Programm von Deep Packet Inspector ist nicht möglich.	Es ist keine Kommunikation zwischen der Integritätsüberwachung und Deep Packet Inspector möglich, um den Status abzurufen. Dies kann bedeuten, dass das Steuerungsprogramm nicht ausgeführt wird, und möglicherweise wird der Netzwerkverkehr nicht durch Nitro IPS geleitet. Möglicherweise können Sie das Problem beheben, indem Sie die Richtlinie erneut anwenden.
Die Systemprotokollierung wird nicht ausgeführt.	Von der Systemprotokollierung wurde keine Antwort erhalten. Möglicherweise können Sie das Problem beheben, indem Sie das Gerät neu starten.
In der Festplattenpartition ist wenig Speicherplatz verfügbar.	Es ist sehr wenig freier Speicherplatz vorhanden.
Warnung zur Lüftergeschwindigkeit	Die Lüfter drehen sich sehr langsam oder gar nicht. Bewahren Sie das Gerät bis zum Austausch des Lüfters in einem Raum mit Klimaanlage auf, um Schäden zu verhindern.

Status	Beschreibung und Anweisungen
Warnung zur Temperatur	Die Temperatur kritischer Komponenten überschreitet einen bestimmten Schwellenwert. Bewahren Sie das Gerät in einem Raum mit Klimaanlage auf, um dauerhafte Schäden zu verhindern. Überprüfen Sie, ob die Luftzirkulation im Gerät blockiert ist.
Netzwerkfehler	Im Netzwerk treten Netzwerkfehler oder übermäßige Kollisionen auf. Dies ist möglicherweise auf eine große Kollisionsdomäne oder fehlerhafte Netzwerkkabel zurückzuführen.
Problem mit einem Remote-Bereitstellungspunkt	Es liegt ein Problem mit einem Remote-Bereitstellungspunkt vor.
Wenig freier Speicherplatz auf Remote-Bereitstellungspunkt	Auf dem Remote-Bereitstellungspunkt ist wenig freier Speicherplatz vorhanden.
Alle Datenquellenerfassungen, die mindestens zehn Minuten lang keine Kommunikation von einer Datenquelle empfangen haben	Der Empfänger hat mindestens zehn Minuten lang keine Kommunikation von einer Datenquelle empfangen.
Die Datenquellenerfassung wird nicht ausgeführt.	Im Subsystem für die Behandlung der spezifischen Drittanbieter-Datenquellen (beispielsweise Syslog oder SNMP) tritt eine Fehlfunktion auf. Die Erfassung hat in einem bestimmten Zeitraum keine Daten von der Drittanbieter-Datenquelle empfangen. Möglicherweise ist die Datenquelle inaktiv, oder es werden nicht wie erwartet Daten an den Empfänger gesendet.
Von der Integritätsüberwachung kann kein gültiger Status aus einem Subsystem abgerufen werden.	Von der Integritätsüberwachung kann kein gültiger Status aus einem Subsystem abgerufen werden.
Wiederherstellung des Subsystems nach dem Status Warnung oder Kritisch	Beim Starten und Anhalten der Integritätsüberwachung wird ein Informationshinweis generiert. Wenn bei der Kommunikation zwischen der Integritätsüberwachung und anderen Subsystemen auf den Geräten Probleme auftreten, wird ebenfalls eine Warnung generiert. Zeigen Sie das Ereignisprotokoll an. Dort finden Sie möglicherweise Details zu den Ursachen der Warnungen vom Typ Warnung und Kritisch.

Löschen einer Gruppe oder eines Geräts

Wenn ein Gerät nicht mehr Bestandteil des Systems ist oder Sie eine Gruppe nicht mehr verwenden, löschen Sie das Gerät bzw. die Gruppe aus der Systemnavigationsstruktur.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Heben Sie in der Systemnavigationsstruktur das zu löschende Gerät bzw. die zu löschende Gruppe hervor, und klicken Sie dann auf der Aktionssymbolleiste auf das Symbol **Löschen**.
2. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **OK**.

Aktualisieren der Geräte

Sie können die Geräte im System manuell aktualisieren, damit ihre Informationen mit denen in ESM übereinstimmen.

- Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Geräte aktualisieren**  .

Konfigurieren von Geräten

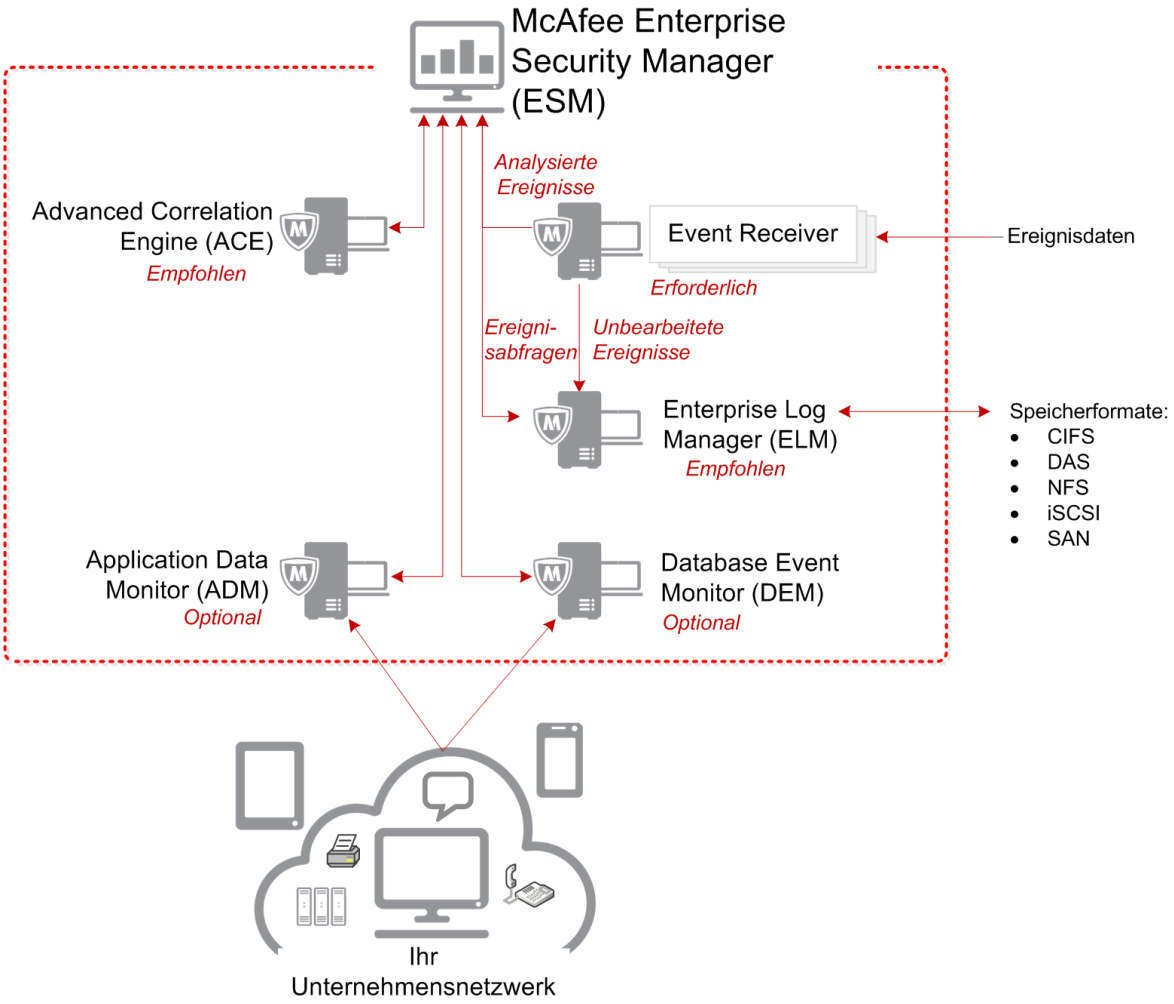
Verbinden Sie physische und virtuelle Geräte mit McAfee ESM, um forensische Funktionen in Echtzeit, Anwendungs- und Datenbanküberwachung, erweiterte regel- und risikobasierte Korrelation sowie die Erstellung von Compliance-Berichten zu ermöglichen.

Inhalt

- *Geräte und ihre Funktion*
- *Event Receiver-Einstellungen*
- *Einstellungen für Enterprise Log Manager (ELM)*
- *Einstellungen für Advanced Correlation Engine (ACE)*
- *Einstellungen für Application Data Monitor (ADM)*
- *Einstellungen für Database Event Monitor (DEM)*
- *Einstellungen für verteilte ESM-Geräte (DESM)*
- *ePolicy Orchestrator-Einstellungen*
- *Einstellungen für Nitro Intrusion Prevention System (Nitro IPS)*
- *McAfee Vulnerability Manager-Einstellungen*
- *McAfee Network Security Manager-Einstellungen*

Geräte und ihre Funktion

Mit dem ESM-Gerät können Sie alle physischen und virtuellen Geräte in einer Sicherheitsumgebung verwalten und mit den Geräten interagieren.



Siehe auch

Event Receiver-Einstellungen auf Seite 63
Einstellungen für Enterprise Log Manager (ELM) auf Seite 120
Einstellungen für Application Data Monitor (ADM) auf Seite 140
Einstellungen für Database Event Monitor (DEM) auf Seite 155
Einstellungen für Advanced Correlation Engine (ACE) auf Seite 136
Einstellungen für verteilte ESM-Geräte (DESM) auf Seite 163
ePolicy Orchestrator-Einstellungen auf Seite 164
Einstellungen für Nitro Intrusion Prevention System (Nitro IPS) auf Seite 170

Event Receiver-Einstellungen

Mit **Event Receiver** können Sie Sicherheitsereignisse und Netzwerk-Flussdaten aus Quellen mehrerer Anbieter erfassen. Dazu gehören unter anderem Firewalls, virtuelle private Netzwerke (VPNs), Router, Nitro IPS und Systeme zur Erkennung von Eindringungsversuchen, NetFlow und sFlow.

Mit **Event Receiver** können Sie diese Daten erfassen und in einer einzigen verwaltbaren Lösung normalisieren. Dadurch erhalten Sie eine einzige Ansicht für Geräte von mehreren Anbietern wie beispielsweise Cisco, Check Point und Juniper. Außerdem können Sie die Ereignis- und Flussdaten von Nitro IPS-Geräten und Routern erfassen, von denen Daten-Feeds an den Empfänger gesendet werden.

Empfänger mit Hochverfügbarkeit (Empfänger-HA) können im primären und im sekundären Modus verwendet werden und dabei als Sicherungen füreinander fungieren. Der primäre Empfänger (A) wird kontinuierlich vom sekundären Empfänger (B) überwacht, und neue Konfigurations- oder Richtlinieninformationen werden an beide Geräte gesendet. Wenn von Empfänger B festgestellt wird, dass auf Empfänger A ein Fehler aufgetreten ist, wird die Netzwerkkarte der Datenquelle von Empfänger A vom Netzwerk getrennt, und Empfänger B ist nun der primäre Empfänger. Er bleibt so lange der primäre Empfänger, bis Sie manuell eingreifen, um Empfänger A als primären Empfänger wiederherzustellen.

Anzeigen von Streaming-Ereignissen

In der **Streaming-Anzeige** wird eine Liste der vom ausgewählten McAfee ePO-Gerät, McAfee® Network Security Manager-Gerät, Empfänger, von der ausgewählten Datenquelle, der ausgewählten untergeordneten Datenquelle oder dem ausgewählten Client generierten Ereignisse angezeigt. Sie können die Liste filtern und ein Ereignis auswählen, um es in einer Ansicht anzuzeigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das anzuzeigende Gerät aus, und klicken Sie dann auf der Aktionssymbolleiste auf das Symbol **Streaming-Ereignisse anzeigen**  .
2. Klicken Sie auf **Starten**, um das Streaming zu starten, und auf **Anhalten**, um es anzuhalten.
3. Wählen Sie eine oder mehrere der verfügbaren Aktionen in der Anzeige aus.
4. Klicken Sie auf **Schließen**.

Empfänger mit Hochverfügbarkeit

Empfänger mit Hochverfügbarkeit werden im primären und im sekundären Modus verwendet, damit die Funktionen schnell vom sekundären Empfänger übernommen werden können, wenn der primäre Empfänger ausfällt. Dadurch wird die Kontinuität der Datenerfassung wesentlich besser gewährleistet als bei einem einzigen Empfänger.



Die Funktion für Empfänger mit Hochverfügbarkeit ist nicht FIPS-konform. Verwenden Sie diese Funktion nicht, wenn Sie FIPS-Vorschriften einhalten müssen.

Dieses Setup besteht aus zwei Empfängern, wobei der eine als primärer oder bevorzugter Empfänger und der andere als sekundärer Empfänger fungiert. Der primäre Empfänger wird kontinuierlich vom sekundären Empfänger überwacht. Wenn vom sekundären Empfänger ein Fehler auf dem primären Empfänger festgestellt wird, wird der primäre Empfänger angehalten und seine Funktion vom sekundären Empfänger übernommen.

Nach der Reparatur des primären Empfängers wird dieser zum sekundären Empfänger oder wieder zum primären Empfänger. Dies hängt davon ab, welche Option auf der Registerkarte **HA-Empfänger** im Feld **Bevorzugtes primäres Gerät** ausgewählt ist (siehe *Einrichten von Empfänger-HA-Geräten*).

Die folgenden Empfängermodelle sind mit der Funktionalität für Hochverfügbarkeit erhältlich:

- ERC-1225-HA
- ERC-2230-HA
- ERC-2250-HA
- ERC-4245-HA
- ERC-4500-HA
- ERC-1250-HA
- ERC-1260-HA
- ERC-2600-HA
- ERC-4600-HA

Diese Modelle verfügen über einen IPMI-Port (Intelligent Platform Management Interface) sowie mindestens vier Netzwerkkarten, die für die HA-Funktionalität benötigt werden (siehe *Netzwerk-Ports an Empfänger-HAs*).

Aufgrund der IPMI-Karten ist es nicht möglich, durch Herunterfahren des Empfängers mit dem Fehler beide DS-Netzwerkkarten mit der freigegebenen IP- und MAC-Adresse gleichzeitig zu verwenden. Die IPMI-Karten sind über ein gekreuztes oder nicht gekreuztes Kabel mit dem jeweils anderen Empfänger verbunden. Die Empfänger sind über ein gekreuztes oder nicht gekreuztes Kabel an der Heartbeat-Netzwerkkarte verbunden. Es gibt eine Verwaltungs-Netzwerkkarte für die Kommunikation mit ESM und eine Datenquellen-Netzwerkkarte für die Erfassung von Daten.

Wenn der primäre Empfänger ordnungsgemäß ausgeführt wird und der sekundäre Empfänger sich im sekundären Modus befindet, geschieht Folgendes:

- Zwischen den Empfängern findet ständig Kommunikation über die dedizierte Heartbeat-Netzwerkkarte und die Verwaltungs-Netzwerkkarte statt.
- Empfangene Zertifikate (beispielsweise für OPSEC oder eStreamer) werden dem jeweils anderen im Paar enthaltenen Empfänger übergeben.
- Von allen Datenquellen wird die Datenquellen-Netzwerkkarte verwendet.
- Auf jedem Empfänger wird die eigene Integrität überwacht, und es werden entsprechende Berichte erstellt. Dazu gehören interne Integritätselemente wie Datenträgerfehler, Einfrieren der Datenbank und getrennte Verbindungen an Netzwerkkarten.
- Status und Integrität der Empfänger werden regelmäßig durch Kommunikation zwischen ESM und den Empfängern ermittelt.
- Neue Konfigurationsinformationen werden sowohl an den primären als auch an den sekundären Empfänger gesendet.
- Richtlinien werden von ESM sowohl an den primären als auch an den sekundären Empfänger gesendet.
- Die Befehle Anhalten, Neu starten, Terminal und Call-Home-Verbindung werden auf jeden Empfänger einzeln angewendet.

In den folgenden Abschnitten wird beschrieben, was bei Problemen auf dem Empfänger-HA geschieht.

Fehler auf dem primären Empfänger

Ob auf dem primären Empfänger ein Fehler vorliegt, wird vom sekundären Empfänger ermittelt. Der Fehler muss schnell und genau ermittelt werden, um den Datenverlust auf ein Minimum zu reduzieren. Beim Failover gehen alle Daten verloren, die hinzugekommen sind, seit letztmals Daten vom primären Empfänger an ESM und das ELM-Gerät gesendet wurden. Der Umfang der verlorenen Daten hängt vom Durchsatz des Empfängers ab sowie von der Rate, mit der über das ESM-Gerät Daten vom Empfänger abgerufen werden. Diese konkurrierenden Prozesse müssen sorgfältig in Einklang miteinander gebracht werden, um die Verfügbarkeit der Daten zu optimieren.

Wenn der primäre Empfänger vollständig ausfällt (Stromausfall, CPU-Fehler), findet keine Heartbeat-Kommunikation mit dem primären Empfänger statt. Der Kommunikationsverlust wird von Corosync erkannt, und der primäre Empfänger wird als fehlgeschlagen markiert. Von Pacemaker auf dem sekundären Empfänger wird das Herunterfahren des primären Empfängers durch dessen IPMI-Karte angefragt. Die freigegebene IP-Adresse und MAC-Adresse werden vom sekundären Empfänger übernommen, und alle Erfassungen werden gestartet.

Fehler auf dem sekundären Empfänger

Das Verfahren für Fehler auf dem sekundären Empfänger wird angewendet, wenn der sekundäre Empfänger nicht mehr auf die Heartbeat-Kommunikation reagiert. Dies bedeutet, dass eine bestimmte Zeit lang keine Kommunikation zwischen dem System und den sekundären Empfänger über die Verwaltungsschnittstelle und die Heartbeat-Schnittstelle möglich war.

Wenn der primäre Empfänger keine Heartbeat-Signale und Integritätssignale empfängt, wird der sekundäre Empfänger von Corosync als fehlgeschlagen markiert und von Pacemaker über seine IPMI-Karte heruntergefahren.

Integritätsproblem auf dem primären Empfänger

Die Integrität des primären Empfängers kann stark beeinträchtigt sein. Zu einer stark kompromittierten Integrität gehören eine nicht reagierende Datenbank, eine nicht regierende Datenquellen-Schnittstelle und übermäßig viele Datenträgerfehler.

Wenn vom primären Empfänger eine Warnung der Integritätsüberwachung für eine dieser Bedingungen bemerkt wird, werden die Corosync- und Pacemaker-Prozesse sofort beendet und eine Warnung der Integritätsüberwachung festgelegt. Durch das sofortige Beenden dieser Prozesse werden die Datenerfassungsaufgaben auf den zweiten Empfänger übertragen.

Integritätsproblem auf dem sekundären Empfänger

Wenn die Integrität des sekundären Empfängers stark beeinträchtigt ist, geschieht Folgendes:

- Vom sekundären Empfänger werden auf Abfrage Integritätsprobleme an ESM gemeldet, und die Corosync- und Pacemaker-Prozesse werden sofort beendet.
- Wenn der sekundäre Empfänger noch Bestandteil des Clusters ist, wird er aus dem Cluster entfernt und ist im Fall eines Fehlers auf dem primären Empfänger nicht verfügbar.
- Das Integritätsproblem wird analysiert, und es wird ein Reparaturversuch unternommen.
- Wenn das Integritätsproblem behoben ist, wird mit dem Verfahren *Wieder in Betrieb nehmen* der Normalbetrieb des Empfängers wieder aufgenommen.
- Wenn das Integritätsproblem nicht behoben ist, wird der Prozess *Ersetzen eines Empfängers mit Fehlern* initiiert.

Wiederinbetriebnahme

Wenn der Empfänger nach einem Fehler wieder in Betrieb genommen wird (beispielsweise Neustart nach einem Stromausfall, einer Hardware-Reparatur oder einer Netzwerkreparatur), geschieht Folgendes:

- Auf Empfängern im Hochverfügbarkeitsmodus wird die Erfassung von Daten beim Starten nicht gestartet. Diese Empfänger bleiben im sekundären Modus, bis sie als primärer Empfänger festgelegt werden.
- Das bevorzugte primäre Gerät übernimmt die Rolle des primären Geräts, und es werden über die freigegebene Datenquellen-IP Daten erfasst. Wenn kein bevorzugtes primäres Gerät vorhanden ist, werden vom aktuellen primären Gerät über die freigegebene Datenquelle Daten erfasst.

Details zu diesem Prozess finden Sie unter *Ersetzen eines Empfängers mit Fehlern*.

Durchführen eines Upgrades auf einem Empfänger-HA

Beim Upgrade-Prozess für Empfänger-HAs wird das Upgrade für beide Empfänger nacheinander, beginnend mit dem sekundären Empfänger, durchgeführt. Dabei geschieht Folgendes:

1. Die Datei mit dem Upgrade-Tarball wird auf das ESM-Gerät hochgeladen und auf den sekundären Empfänger angewendet.
2. Sie wechseln die Rolle des primären und sekundären Empfängers und verwenden dabei den Prozess zum *Wechseln zwischen Empfänger-HA-Rollen*. Der Empfänger, für den Sie das Upgrade durchgeführt haben, ist nun der primäre Empfänger, und der Empfänger, für den noch kein Upgrade durchgeführt wurde, ist der sekundäre Empfänger.
3. Der Upgrade-Tarball wird auf den neuen sekundären Empfänger angewendet.
4. Sie wechseln erneut die Rollen des primären und sekundären Empfängers mit dem Prozess zum *Wechseln zwischen Empfänger-HA-Rollen*, sodass die Empfänger wieder ihre ursprünglichen Rollen annehmen.

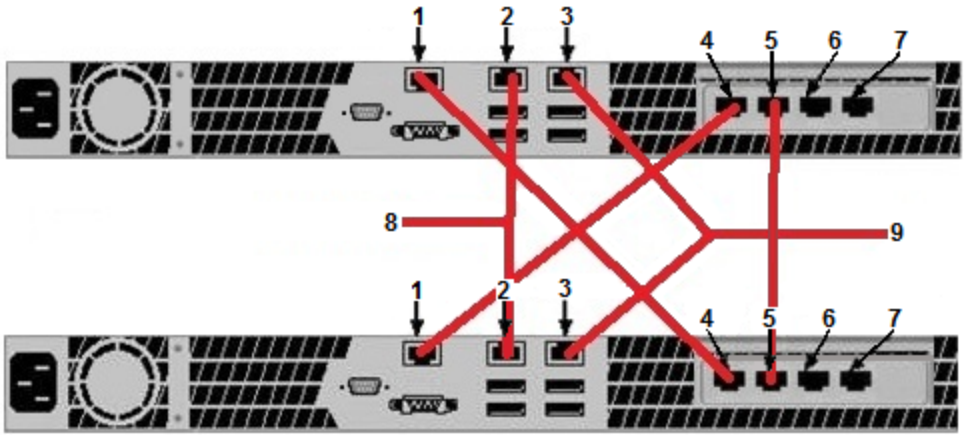
Beim Durchführen von Upgrades sollte kein bevorzugter primärer Empfänger festgelegt sein. Weitere Informationen finden Sie unter

Wenn für den Empfänger-HA ein bevorzugter primärer Empfänger eingerichtet ist, ändern Sie am besten die Einstellung vor dem Upgrade. Wählen Sie auf der Registerkarte **HA-Empfänger** (siehe *Einrichten von Empfänger-HA-Geräten*) im Feld **Bevorzugtes primäres Gerät** die Option **Keine** aus. Auf diese Weise können Sie die Option **Failover** verwenden, die nicht verfügbar ist, wenn Sie die Einstellung als bevorzugtes primäres Gerät ausgewählt haben. Wenn das Upgrade für beide Empfänger durchgeführt wurde, können Sie die Einstellung als bevorzugtes primäres Gerät wieder anwenden.

Netzwerk-Ports an Empfänger-HAs

In den folgenden Diagrammen wird gezeigt, wie Sie die Netzwerk-Ports an einem Empfänger-HA verbinden.

ERC-1250-HA/1260-HA



1. IPMI
2. Verwaltung 2
6. Verwaltung 2
7. Verwaltung 3

3 Verwaltung 1

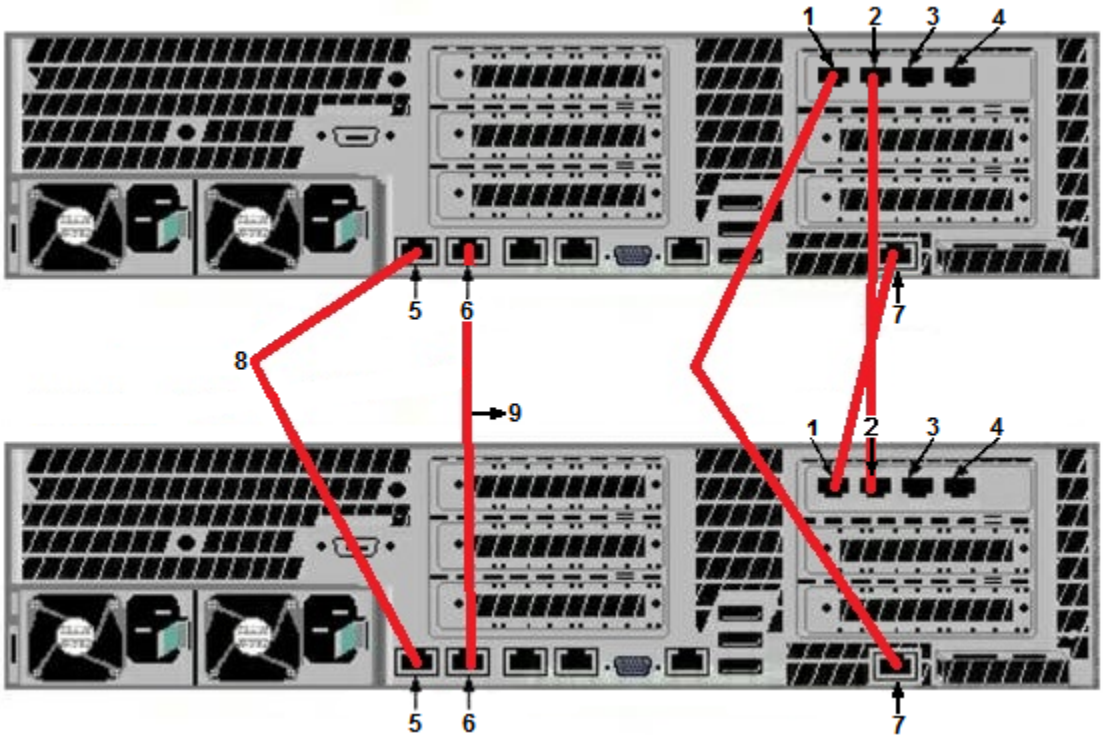
4 IPMI-Netzwerkkarte

5 Heartbeat (HB)

8 Daten-Feed

9 Verwaltung 1 IP

ERC-2600-HA und ERC-4600-HA



1 IPMI-Netzwerkkarte

2 HB

3 Verwaltung 2

4 Verwaltung 3

5 Verwaltung

6 Daten

7 IPMI

8 Verwaltung 1

9 Daten-Feed

Einrichten von Empfänger-HA-Geräten

Definieren Sie die Einstellungen für die Empfänger-HA-Geräte.

Bevor Sie beginnen

Fügen Sie den als primäres Gerät verwendeten Empfänger hinzu (siehe *Hinzufügen von Geräten zur ESM-Konsole*). Der Empfänger muss über mindestens drei Netzwerkkarten verfügen.

Die Funktion für Empfänger mit Hochverfügbarkeit ist nicht FIPS-konform. Verwenden Sie diese Funktion nicht, wenn Sie FIPS-Vorschriften einhalten müssen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur den Empfänger aus, der als primäres HA-Gerät verwendet werden soll. Klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Empfängerkonfiguration** und dann auf **Schnittstelle**.
3. Klicken Sie auf die Registerkarte **HA-Empfänger**, und wählen Sie dann **Hochverfügbarkeit einrichten** aus.
4. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Damit initiieren Sie den Prozess, bei dem der Schlüssel für den zweiten Empfänger festgelegt wird, aktualisieren die Datenbank, wenden `globals.conf` an und synchronisieren die beiden Empfänger.

Erneutes Initialisieren des sekundären Geräts

Wenn der sekundäre Empfänger aus irgendeinem Grund außer Betrieb genommen wird, müssen Sie nach der erneuten Installation erneut initialisieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** für den primären Empfänger aus, und klicken Sie dann auf **Empfängerkonfiguration** | **Schnittstelle** | **HA-Empfänger**.
2. Vergewissern Sie sich, dass im Feld **Sekundäre Verwaltungs-IP** die richtige IP-Adresse eingetragen ist.
3. Klicken Sie auf **Sekundären Empfänger erneut initialisieren**.

Von ESM werden die notwendigen Schritte zum erneuten Initialisieren des Empfängers ausgeführt.

Zurücksetzen von HA-Geräten

Wenn Sie HA-Empfänger auf den Zustand vor der Einrichtung als HA-Geräte zurücksetzen müssen, können Sie die ESM-Konsole oder, falls keine Kommunikation mit den Empfängern möglich ist, dass LCD-Menü verwenden.

- Führen Sie einen der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Zurücksetzen eines Empfängers in der ESM-Konsole	1 Klicken Sie in der Systemnavigationsstruktur auf die Option **Empfängereigenschaften**, und klicken Sie dann auf **Empfängerkonfiguration** | **Schnittstelle**. 2 Heben Sie die Auswahl von **Hochverfügbarkeit einrichten** auf, und klicken Sie dann auf **OK**. 3 Klicken Sie auf der Warnungsseite auf **Ja**, und klicken Sie dann auf **Schließen**. Nach einer Zeitüberschreitung von etwa fünf Minuten werden beide Empfänger erneut gestartet und die MAC-Adressen auf die ursprünglichen Werte zurückgesetzt.
Zurücksetzen des primären oder sekundären Empfängers im LCD-Menü	1 Drücken Sie im LCD-Menü des Empfängers auf **X**. 2 Drücken Sie den Pfeil nach unten, bis **Disable HA** angezeigt wird. 3 Drücken Sie einmal den Pfeil nach rechts, um auf dem LCD-Bildschirm die Option **Disable Primary** anzuzeigen. 4 Zum Zurücksetzen des primären Empfängers drücken Sie das Häkchen. 5 Zum Zurücksetzen des sekundären Empfängers drücken Sie einmal den Pfeil nach unten und dann das Häkchen.

Wechseln zwischen Empfänger-HA-Rollen

Mithilfe des vom Benutzer initiierten Wechselprozesses können Sie zwischen den Rollen des primären und sekundären Empfängers wechseln.

Möglicherweise müssen Sie so vorgehen, wenn Sie ein Upgrade für einen Empfänger durchführen, einen Empfänger für die Rücksendung an den Hersteller vorbereiten oder Kabel an einem Empfänger umstecken. Bei diesem Wechsel wird die Menge der verlorenen Daten auf ein Minimum reduziert.



Wenn eine Erfassung (einschließlich des McAfee ePO-Geräts) einem Empfänger-HA zugeordnet ist und für den Empfänger-HA ein Failover ausgeführt wird, ist die Kommunikation zwischen der Erfassung und dem Empfänger-HA erst wieder möglich, wenn auf den Switches zwischen den beiden die neue MAC-Adresse des Empfängers, für den ein Failover ausgeführt wurde, der freigegebenen IP-Adresse zugeordnet wurde. Abhängig von der aktuellen Netzwerkkonfiguration kann dies ein paar Minuten oder auch mehrere Tage dauern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das Empfänger-HA-Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Wählen Sie Folgendes aus: **Hochverfügbarkeit** | **Failover**. Folgendes geschieht:

- Der sekundäre Empfänger wird von ESM angewiesen, die freigegebene Datenquellen-IP zu verwenden und Daten zu erfassen.
- Auf dem sekundären Empfänger wird ein CRM-Befehl (Cluster Resource Manager) ausgegeben, um die freigegebene IP- und MAC-Adresse zu wechseln, und die Erfassungen werden gestartet.
- Auf dem ESM-Geräte werden alle Warnungs- und Flussdaten vom primären Empfänger abgerufen.
- Der sekundäre Empfänger wird vom ESM-Gerät als primärer Empfänger markiert, und der primäre Empfänger wird als sekundärer Empfänger markiert.

Durchführen eines Upgrades für HA-Empfänger

Beim Upgrade-Prozess für Empfänger-HAs wird das Upgrade für beide Empfänger nacheinander, beginnend mit dem sekundären Empfänger, durchgeführt.

Lesen Sie sich vor dem Starten des Upgrade-Prozesses den Abschnitt *Überprüfen des Hochverfügbarkeitsstatus eines Empfängers* durch, um sicherzustellen, dass die Empfänger-HA-Geräte für das Upgrade bereit sind. Wenn Sie dies nicht tun, kann es zu Problemen beim Upgrade des Geräts und zu Ausfallzeiten kommen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das Empfänger-HA-Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Führen Sie das Upgrade für den sekundären Empfänger durch:

   a Klicken Sie auf **Empfängerverwaltung**, und wählen Sie dann **Sekundär** aus.

   b Klicken Sie auf **Gerät aktualisieren**, und wählen Sie dann die zu verwendende Datei aus, oder navigieren Sie zu der Datei. Klicken Sie auf **OK**.

   Der Empfänger wird neu gestartet, und die Version der Software wird aktualisiert.

   c Klicken Sie in **Empfängereigenschaften** auf **Hochverfügbarkeit** | **Wieder in Betrieb nehmen**.

   d Wählen Sie den sekundären Empfänger aus, und klicken Sie dann auf **OK**.

3 Ändern Sie den sekundären Empfänger in den primären Empfänger, indem Sie auf Folgendes klicken: **Hochverfügbarkeit** | **Failover**.

4 Führen Sie das Upgrade für den neuen sekundären Empfänger durch, indem Sie Schritt 2 wiederholen.

Überprüfen des Hochverfügbarkeitsstatus eines Empfängers

Ermitteln Sie den Status eines HA-Empfängerpaars, bevor Sie ein Upgrade durchführen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das primäre Empfänger-HA-Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Vergewissern Sie sich in den Feldern **Status** und **Sekundärer Status**, dass der Status **OK**, **HA-Status: online** lautet.

3 Greifen Sie über Secure Shell oder SSH auf die einzelnen HA-Empfänger zu, und führen Sie auf beiden Empfängern über die Befehlszeilenschnittstelle den Befehl `ha_status` aus. Aus den daraufhin angezeigten Informationen geht der Status des Empfängers sowie der vom Empfänger angenommene Status des anderen Empfängers hervor. Die Informationen sehen in etwa so aus:

```
OK
Hostname=McAfee1
Modus=Primär
McAfee1=Online
McAfee2=Online
sharedIP=McAfee1
stonith=McAfee2
corosync=Wird ausgeführt
hi_bit=Nein
```

4 Vergewissern Sie sich oben, dass Folgendes zutrifft:

- Die erste Zeile der Antwort lautet `OK`.
- `Hostname` stimmt mit dem Hostnamen auf der Befehlszeile ohne die Modellnummer des Empfängers überein.
- `Modus` entspricht Primär, wenn der Wert von `sharedIP` der Hostname dieses Empfängers ist. Anderenfalls lautet der Modus Sekundär.
- In den nächsten beiden Zeilen werden die Hostnamen der Empfänger im HA-Paar angezeigt und der Ausführungsstatus der einzelnen Empfänger aufgeführt. Der Status für beide lautet **Online**.
- Mit `corosync=` wird der Ausführungsstatus von Corosync angezeigt, der Wird ausgeführt entsprechen sollte.
- `hi_bit` entspricht auf dem einen Empfänger `Nein` und auf dem anderen `Ja`. Um welchen Empfänger es sich jeweils handelt, spielt dabei keine Rolle.



Stellen Sie sicher, dass nur für einen der HA-Empfänger der hi_bit-Wert festgelegt ist. Wenn für beide HA-Empfänger der gleiche Wert festgelegt ist, wenden Sie sich vor der Durchführung des Upgrades an den McAfee-Support, um die falsch konfigurierte Einstellung zu korrigieren.

5 Greifen Sie über Secure Shell oder SSH auf die einzelnen HA-Empfänger zu, und führen Sie auf beiden Empfängern über die Befehlszeilenschnittstelle den Befehl `ifconfig` aus.

6 Vergewissern Sie sich, dass Folgendes auf die generierten Daten zutrifft:

- Die MAC-Adressen an eth0 und eth1 sind auf beiden Empfängern eindeutig.
- Der primäre Empfänger hat die freigegebene IP-Adresse an eth1, und der sekundäre Empfänger hat keine IP-Adresse an eth1.

  Wenn für beide HA-Empfänger der gleiche Wert festgelegt ist, wenden Sie sich vor der Durchführung des Upgrades an den McAfee-Support, um die falsch konfigurierte Einstellung zu korrigieren.

Mit dieser Stichprobe stellen Sie sicher, dass das System funktionsfähig ist und dass keine doppelten IP-Adressen vorhanden sind. Dies bedeutet, dass Sie das Upgrade durchführen können.

Ersetzen eines Empfängers mit Fehlern

Wenn auf einem sekundären Empfänger ein Integritätsproblem besteht, das nicht behoben werden kann, müssen Sie möglicherweise den Empfänger ersetzen. Wenn Sie den neuen Empfänger erhalten haben, installieren Sie ihn gemäß den Verfahren in *McAfee ESM – Einrichtungs- und Installationshandbuch*. Wenn die IP-Adressen festgelegt und die Kabel angeschlossen sind, können Sie den Empfänger wieder in den HA-Cluster aufnehmen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** für den HA-Empfänger aus, und klicken Sie dann auf **Empfängerkonfiguration** | **Schnittstelle**.
2. Klicken Sie auf die Registerkarte **HA-Empfänger**, und vergewissern Sie sich dann, dass **Hochverfügbarkeit einrichten** ausgewählt ist.
3. Überprüfen Sie die IP-Adressen, und klicken Sie dann auf **Sekundären Empfänger erneut initialisieren**.

Der neue Empfänger wird in den Cluster aufgenommen, und der HA-Modus wird aktiviert.

Fehlerbehebung für Empfänger mit Fehlern

Wenn ein Empfänger in einer HA-Konfiguration aus irgendeinem Grund ausfällt, schlägt das Schreiben von Datenquellen, globalen Einstellungen, Aggregationseinstellungen und anderen Informationen fehl, und ein SSH-Fehler wird angezeigt.

Tatsächlich wird ein Rollout für die Einstellungen auf dem noch funktionierenden Empfänger ausgeführt. Da jedoch die Synchronisierung mit dem ausgefallenen Empfänger nicht möglich ist, wird eine Fehlermeldung angezeigt. Für Richtlinien wird jedoch kein Rollout ausgeführt. In dieser Situation stehen folgende Optionen zur Verfügung:

- Warten Sie mit dem Rollout für Richtlinien, bis ein sekundärer Empfänger verfügbar ist und synchronisiert wurde.
- Deaktivieren Sie den HA-Modus auf dem Empfänger. Dadurch entsteht eine Ausfallzeit von zwei bis fünf Minuten für den HA-Cluster, während der keine Ereignisse gesammelt werden.

Archivieren von Rohdaten für Empfänger

Konfigurieren Sie den Empfänger für die Weiterleitung einer Sicherung der Rohdaten an das Speichergerät zur langfristigen Speicherung.

Von ESM werden die folgenden drei Speichertypen unterstützt: Server Message Block/Common Internet File System (SMB/CIFS), Network File System (NFS) und Syslog-Weiterleitung. Bei SMB/CIFS und NFS wird eine Sicherung aller von Datenquellen an den Empfänger gesendeten Rohdaten in Form von Datendateien gespeichert. Dies gilt für Daten, die mit E-Mail-, Estream-, HTTP-, SNMP-, SQL-, Syslog- und Remote-Agent-Protokollen gesendet wurden. Diese Datendateien werden alle fünf Minuten an das Archiv gesendet. Bei der Syslog-Weiterleitung werden die Rohdaten für Syslog-Protokolle als kontinuierlicher Stream aus kombinierten Syslogs an das Gerät gesendet, das Sie auf der Seite **Einstellungen für die Datenarchivierung** im Abschnitt **Syslog-Weiterleitung** konfiguriert haben. Vom Empfänger kann nur jeweils ein Speichertyp weitergeleitet werden. Sie können alle drei Typen konfigurieren, jedoch kann nur ein Typ für das Archivieren von Daten aktiviert sein.

Die Datenquellentypen Netflow, sflow und IPFIX werden von dieser Funktion nicht unterstützt.

Definieren von Archiveinstellungen

Zum Speichern der Rohdaten von Syslog-Nachrichten müssen Sie die Einstellungen konfigurieren, die vom Empfänger für die Archivierung verwendet werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Empfängerkonfiguration** | **Datenarchivierung**.

2 Wählen Sie den Freigabetyp aus, und geben Sie die erforderlichen Informationen ein.



Auf dem System mit der CIFS-Freigabe müssen Sie Port 445 öffnen, um eine Verbindung mit der CIFS-Freigabe zu ermöglichen. Entsprechend muss auf dem System mit der SMB-Freigabe Port 135 geöffnet werden, damit eine SMB-Verbindung hergestellt werden kann.

3 Wenn Sie bereit sind, die Änderungen auf das Empfängergerät anzuwenden, klicken Sie auf **OK**.

Anzeigen von Quellereignissen für Korrelationsereignisse

In der Ansicht **Ereignisanalyse** können Sie die Quellereignisse für ein Korrelationsereignis anzeigen.

Bevor Sie beginnen

Auf dem ESM-Gerät muss bereits eine Korrelationsdatenquelle vorhanden sein (siehe *Korrelationsdatenquelle* und *Hinzufügen einer Datenquelle*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Erweitern Sie in der Systemnavigationsstruktur den Empfänger, und klicken Sie dann auf **Korrelationsmodul**.

2 Klicken Sie in der Liste der Ansichten auf **Ereignisansichten**, und wählen Sie dann **Ereignisanalyse** aus.

3 Klicken Sie in der Ansicht **Ereignisanalyse** auf das Pluszeichen (+) in der ersten Spalte neben dem Korrelationsereignis.



Ein Pluszeichen wird nur angezeigt, wenn das Korrelationsereignis über Quellereignisse verfügt.

Die Quellereignisse werden unter dem Korrelationsereignis aufgeführt.

Anzeigen der Durchsatzstatistik für Empfänger

Zeigen Sie eine Verwendungsstatistik für Empfänger an. Diese enthält unter anderem die eingehenden (Erfassung) und ausgehenden (Analyse) Datenquellenraten der letzten zehn Minuten, der letzten Stunde und der letzten 24 Stunden.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie über die Berechtigung zur Geräteverwaltung verfügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur einen Empfänger aus, und klicken Sie dann auf das Symbol Eigenschaften .
2. Klicken Sie auf **Empfängerverwaltung | Statistik anzeigen | Durchsatz**.
3. Zeigen Sie die Empfängerstatistik an.

   Wenn die eingehenden Raten die Ausgaberate um 15 Prozent überschreiten, wird die entsprechende Zeile vom System als kritisch (in den letzten 24 Stunden) oder als Warnung (in der letzten Stunde) gekennzeichnet.
4. Filtern Sie die Datenquelle, indem Sie die Option Alle, Kritisch oder Warnung auswählen.
5. Wählen Sie die Maßeinheit zum Anzeigen der Messgrößen aus: nach der Anzahl der Kilobytes (KBs) oder nach der Anzahl der Datensätze.
6. Wenn die Daten automatisch alle zehn Sekunden aktualisiert werden sollen, aktivieren Sie das Kontrollkästchen **Automatisch aktualisieren**.
7. Sortieren Sie die Daten, indem Sie auf den entsprechenden Spaltentitel klicken.

Empfängerdatenquellen

Mit McAfee Event Receiver können Sie Sicherheitsereignisse und Netzwerk-Flussdaten aus Quellen mehrerer Anbietern erfassen. Dazu gehören unter anderem Firewalls, virtuelle private Netzwerke (VPNs), Router, Nitro IPS/IDS, NetFlow und sFlow. Mithilfe von Datenquellen steuern Sie, auf welche Weise die Protokoll- und Ereignisdaten vom Empfänger gesammelt werden. Sie müssen Datenquellen hinzufügen und ihre Einstellungen definieren, damit die gewünschten Daten erfasst werden.

Die Seite **Datenquellen** bildet den Ausgangspunkt für die Verwaltung der Datenquellen für das Empfängergerät. Hier können Sie Datenquellen hinzufügen, bearbeiten und löschen sowie importieren, exportieren und migrieren. Außerdem können Sie untergeordnete Datenquellen und Client-Datenquellen hinzufügen.

Hinzufügen einer Datenquelle

Konfigurieren Sie die Einstellungen für die Datenquellen, die Sie zum Empfänger hinzufügen müssen, um Daten zu erfassen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur den Empfänger aus, zu dem Sie die Datenquelle hinzufügen möchten, und klicken Sie dann auf das Symbol **Eigenschaften** .
2. Klicken Sie in **Empfängereigenschaften** auf **Datenquellen | Hinzufügen**.
3. Wählen Sie den Anbieter und das Modell aus.

   Welche Felder Sie ausfüllen, hängt von Ihrer Auswahl ab.
4. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Die Datenquelle wird zur Liste der Datenquellen auf dem Empfänger sowie zur Systemnavigationsstruktur unter dem ausgewählten Empfänger hinzugefügt.

Verarbeiten einer Datenquelle mit SNMP-Trap

Bei Verwendung der SNMP-Trap-Funktion können von einer Datenquelle standardmäßige SNMP-Traps von jedem verwaltbaren Netzwerkgerät akzeptiert werden, von dem SNMP-Traps gesendet werden können.

Es handelt sich um die folgenden Standard-Traps:

- Fehlgeschlagene Authentifizierung
- Kaltstart
- Verlust des EGP-Nachbarn
- Verbindung inaktiv
- Verbindung aktiv und Warmstart

Zum Senden von SNMP-Traps über IPv6 müssen Sie die IPv6-Adresse als IPv4-Konvertierungsadresse formulieren. Die Konvertierung von 10.0.2.84 in IPv6 würde beispielsweise wie folgt aussehen:

2001:470:B:654:0:0:10.0.2.84 oder 2001:470:B:654::A000:0254.

Wenn Sie **SNMP-Trap** auswählen, stehen drei Optionen zur Verfügung:

- Wenn noch kein Profil ausgewählt ist, wird das Dialogfeld **SNMP-Datenquellenprofile** geöffnet, in dem Sie das gewünschte Profil auswählen können.
- Wenn bereits ein Profil ausgewählt ist, wird das Dialogfeld **SNMP-Datenquellenprofile** geöffnet. Zum Ändern des Profils klicken Sie im Feld **Systemprofile** auf den Pfeil nach unten, und wählen Sie ein neues Profil aus.
- Wenn bereits ein Profil ausgewählt ist, das Sie ändern möchten, und das gewünschte Profil nicht in der Dropdown-Liste im Dialogfeld **SNMP-Datenquellenprofile** enthalten ist, erstellen Sie ein Datenquellen-SNMP-Profil.

Verwalten von Datenquellen

Auf der Seite **Datenquellen** können Sie Datenquellen hinzufügen, bearbeiten, löschen, importieren, exportieren und migrieren sowie untergeordnete Datenquellen und Client-Datenquellen hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquellen**.
2. Zeigen Sie eine Liste der Datenquellen auf dem Empfänger an, und führen Sie eine oder mehrere der verfügbaren Optionen zum Verwalten der Datenquellen aus.
3. Klicken Sie auf **Anwenden** oder **OK**.

SIEM Collector

Von SIEM Collector werden Windows-Ereignisprotokolle über eine verschlüsselte Verbindung an einen Empfänger gesendet.

Ohne SIEM Collector können Windows-Ereignisse nur mithilfe des WMI-Protokolls oder eines Agenten eines Drittanbieters erfasst werden. In vielen Umgebungen ist der Zugriff auf das System durch Sicherheitsrichtlinien gesperrt, sodass Sie WMI nicht verwenden können.

Der WMI-Datenverkehr besteht aus Klartext und ermöglicht nur den Zugriff auf Protokolle, die in das Windows-Ereignisprotokoll geschrieben wurden. Sie können nicht auf Protokolldateien zugreifen, die von anderen Diensten wie beispielsweise DNS, DHCP und IIS oder mithilfe eines anderen Agenten eines Drittanbieters erstellt wurden.

Indem Sie SIEM Collector als eigenständige Anwendung oder als Teil einer vorhandenen McAfee ePolicy Orchestrator-Implementierung verwenden, können Sie die WMI-Funktionalität zu vorhandenen Instanzen von McAfee Agent hinzufügen.

Sie können SIEM Collector auch als Hub verwenden, um über RPC Protokolle von anderen Systemen zu erfassen, ohne das SIEM Collector-Paket zu jedem einzelnen System hinzuzufügen.

Außerdem sind die folgenden Funktionen enthalten:

- Plug-In für benutzerdefinierte SQL-Datenbankerfassung (mit Unterstützung für SQL Server und Oracle)
- Plug-In für das Analysieren exportierter Windows-Ereignisse im EVT- oder EVTX-Format
- Plug-In für die Unterstützung von SQL Server C2-Audits (TRC-Format)

Integrieren von Vulnerability Assessment-Daten

Mit Vulnerability Assessment (VA) auf dem DEM-Gerät und dem Empfänger können Sie Daten integrieren, die von vielen VA-Anbietern abgerufen werden können.

Sie haben verschiedene Möglichkeiten, diese Daten zu verwenden.

- Erhöhen Sie den Schweregrad eines Ereignisses basierend auf der bekannten Schwachstelle des Endpunkts in Bezug auf dieses Ereignis.
- Legen Sie fest, dass Ressourcen und deren Attribute (entdeckte Betriebssysteme und Dienste) automatisch vom System erlernt werden.
- Erstellen und ändern Sie die Mitgliedschaft in benutzerdefinierten Ressourcengruppen.
- Greifen Sie auf zusammengefasste Informationen und nach weiteren Details aufgegliederte Informationen zu den Netzwerkressourcen zu.
- Ändern Sie die **Richtlinien-Editor**-Konfiguration, indem Sie beispielsweise MySQL-Signaturen aktivieren, wenn eine Ressource erkannt wird, auf der MySQL ausgeführt wird.

Sie können in vordefinierten Ansichten oder selbst erstellten benutzerdefinierten Ansichten auf vom System generierte VA-Daten zugreifen. Die folgenden vordefinierten Ansichten sind vorhanden:

- **Dashboard-Ansichten | Dashboard für Ressourcenschwachstellen**
- **Compliance-Ansichten | PCI | Testen von Sicherheitssystemen und -prozessen | 11.2 Schwachstellen-Scans im Netzwerk**
- **Management-Ansichten | Kritische Schwachstellen in regulierten Ressourcen**

Informationen zum Erstellen einer benutzerdefinierten Ansicht finden Sie unter *Hinzufügen einer benutzerdefinierten Ansicht*.



Wenn Sie eine Ansicht erstellen, die die Komponenten **Anzahl der Schwachstellen insgesamt**, **Anzahl** oder **Messuhr** enthält, wird möglicherweise eine zu hohe Anzahl von Schwachstellen angezeigt. Dies liegt daran, dass durch den Feed von McAfee Threat Intelligence Services (MTIS) Bedrohungen basierend auf der von der VA-Quelle gemeldeten ursprünglichen Schwachstelle hinzugefügt werden (siehe *Bewertung von Ressourcen, Bedrohungen und Risiken*).

Das für Regeln zuständige McAfee-Team verwaltet eine Regeldatei, in der eine McAfee-Signatur-ID einer VIN, mindestens einem Verweis auf eine CVE-ID (Common Vulnerabilities and Exposures), BugTraq-ID, OSVDB-ID (Open Source Vulnerability Database) und/oder Secunia-ID zugeordnet wird. Diese Anbieter melden CVE- und BugTraq-IDs in ihren Schwachstellen. Daher sind CVE- und BugTraq-IDs in dieser Version enthalten.

Definieren eines VA-Systemprofils

Beim Hinzufügen einer eEye REM-Quelle haben Sie auf der Seite **Vulnerability Assessment-Quelle hinzufügen** die Möglichkeit, ein bereits definiertes Systemprofil hinzuzufügen. Um diese Funktion zu verwenden, müssen Sie zuerst das Profil definieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein DEM-Gerät oder ein Empfängergerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Vulnerability Assessment** | **Hinzufügen**.
3. Wählen Sie im Feld **Typ der VA-Quelle** die Option **eEye REM** aus.
4. Klicken Sie auf **Systemprofil verwenden**.
5. Klicken Sie auf **Hinzufügen**, und wählen Sie dann im Feld **Profiltyp** die Option **Vulnerability Assessment** aus.
6. Wählen Sie im Feld **Profil-Agent** die SNMP-Version für das Profil aus.

   Die Felder auf der Seite werden abhängig von der ausgewählten Version aktiviert.
7. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Hinzufügen einer VA-Quelle

Für die Kommunikation mit VA-Quellen müssen Sie die Quelle zum System hinzufügen, Kommunikationsparameter für den VA-Anbieter konfigurieren, Parameter planen, mit denen Sie die Häufigkeit des Datenabrufs vorschreiben, und Berechnungen des Ereignisschweregrads ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein DEM-Gerät oder ein Empfängergerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Vulnerability Assessment**.
3. Sie können VA-Quellen hinzufügen, bearbeiten, entfernen oder abrufen und Änderungen in das Gerät schreiben.
4. Klicken Sie auf **Anwenden** oder **OK**.

Abrufen von VA-Daten

Wenn Sie eine Quelle hinzugefügt haben, können Sie die VA-Daten abrufen. Sie haben zwei Möglichkeiten, VA-Daten aus einer Quelle abzurufen: geplant oder sofort. Beide Abrufarten sind für alle VA-Quellen mit Ausnahme von eEye REM möglich (bei eEye REM muss der Abruf geplant werden).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **DEM** oder **Empfängereigenschaften** aus, und klicken Sie dann auf **Vulnerability Assessment**.
2. Wählen Sie die VA-Quelle und dann eine der folgenden Optionen aus.

Aufgabe	Vorgehensweise
Sofortiges Abrufen	• Klicken Sie auf **Abrufen**. Der Auftrag wird im Hintergrund ausgeführt. Wenn der Abruf erfolgreich war, werden Sie informiert (anderenfalls finden Sie weitere Informationen unter *Fehlerbehebung für den VA-Abruf*).
Planen des Abrufs	1 Klicken Sie auf **Bearbeiten**. 2 Wählen Sie im Feld **VA-Datenabruf planen** die Häufigkeit aus. 3 Klicken Sie auf **OK**. 4 Klicken Sie auf der Seite **Vulnerability Assessment** auf **Schreiben**, um die Änderungen in das Gerät zu schreiben.

3 Klicken Sie auf **OK**.

4 Zum Anzeigen der Daten klicken Sie auf das Schnellstartsymbol für **Asset Manager**  , und wählen Sie dann die Registerkarte **Vulnerability Assessment** aus.

Fehlerbehebung für den VA-Abruf

Beim Abrufen von VA-Daten werden Sie informiert, falls der Vorgang nicht erfolgreich ausgeführt wurde. Die folgenden Gründe sind unter anderem möglich, wenn der Abruf nicht erfolgreich ausgeführt wurde.

Ressource	Verursachtes Problem
Nessus, OpenVAS und Rapid7 Metasploit Pro	• Leeres Verzeichnis • Fehler in den Einstellungen • Die Daten im Verzeichnis wurden bereits abgerufen, daher sind die Daten nicht aktuell.
Qualys, FusionVM und Rapid7 Nexpose	Die Daten im Verzeichnis wurden bereits abgerufen, daher sind die Daten nicht aktuell.
Nessus	Wenn Sie beim Hochladen einer neuen Nessus-Datei auf Ihre FTP-Site eine vorhandene Nessus-Datei überschrieben haben, bleibt das Datum der Datei unverändert. Daher werden beim Ausführen eines VA-Abrufs keine Daten zurückgegeben, da die Daten als alte Daten betrachtet werden. Diese Situation können Sie vermeiden, indem Sie die alte Nessus-Datei auf der FTP-Site vor dem Hochladen der neuen Datei löschen oder für die hochgeladene Datei einen anderen Namen verwenden.

Verfügbare VA-Anbieter

Die folgenden VA-Anbieter können in ESM integriert werden.

VA-Anbieter	Version
Digital Defense Frontline	5.1.1.4
eEye REM (REM Events Server)	3.7.9.1721

VA-Anbieter	Version
eEye Retina  Die VA-Quelle von eEye Retina ist mit der Nessus-Datenquelle vergleichbar. Sie können auswählen, ob die RTD-Dateien über SCP, FTP, NFS oder CIFS abgerufen werden sollen. Sie müssen die RTD-Dateien manuell in eine SCP-, FTP- oder NFS-Freigabe kopieren, um sie abzurufen. Die RTD-Datei befinden sich normalerweise im Verzeichnis Retina Scans.	5.13.0, Audits: 2400
McAfee Vulnerability Manager	6.8, 7.0
Critical Watch FusionVM	4-2011.6.1.48
LanGuard	10.2
Lumension	Unterstützung für PatchLink Security Management Console 6.4.5 und höher
nCircle	6.8.1.6
Nessus	Unterstützung für Tenable Nessus, Versionen 3.2.1.1 und 4.2, sowie die Dateiformate NBE, .nessus (XMLv2) und .nessus (XMLv1), außerdem für das XML-Format von OpenNessus 3.2.1
NGS	
OpenVAS	3.0, 4.0
Qualys	
Rapid7 Nexpose	
Rapid7 Metasploit Pro  Sie können den Schweregrad eines Metasploit-Exploits, der mit dem Namen Nexpose beginnt, ableiten, indem Sie zum gleichen Empfänger eine Rapid7-VA-Quelle hinzufügen. Wenn der Schweregrad nicht abgeleitet werden kann, wird der Standardschweregrad 100 verwendet.	4.1.4 Update 1, Dateiformat XML
Saint	

Automatisches Erstellen von Datenquellen

Sie können den Empfänger so einrichten, dass Datenquellen automatisch erstellt werden. Dabei werden die fünf im Lieferumfang des Empfängers enthaltenen Standardregeln oder von Ihnen erstellte Regeln verwendet.

Bevor Sie beginnen

Stellen Sie sicher, dass die automatische Überprüfung im Dialogfeld **Ereignisse, Flüsse und Protokolle** (**Systemeigenschaften | Ereignisse, Flüsse und Protokolle**) aktiviert ist, oder klicken Sie auf der Aktionssymbolleiste auf das Symbol **Ereignisse und Flüsse abrufen**  , um Ereignisse und/oder Flüsse abzurufen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in **Empfängereigenschaften** auf **Datenquellen | Automatisch lernen**.
2. Klicken Sie im Fenster **Automatisch lernen** auf **Konfigurieren**.
3. Stellen Sie im Fenster **Editor für automatisch hinzugefügte Regeln** sicher, dass **Automatische Erstellung von Datenquellen aktivieren** ausgewählt ist. Wählen Sie dann die Regeln für automatisches Hinzufügen aus, die vom Empfänger zum automatischen Erstellen von Datenquellen verwendet werden sollen.
4. Klicken Sie auf **Ausführen**, wenn Sie die ausgewählten Regeln auf die vorhandenen automatisch erlernten Daten anwenden möchten. Klicken Sie dann auf **Schließen**.

Hinzufügen neuer Regeln für automatisches Erstellen

Sie können benutzerdefinierte Regeln hinzufügen, die vom Empfänger für das automatische Erstellen von Datenquellen verwendet werden sollen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in **Empfängereigenschaften** auf **Datenquellen | Automatisch lernen | Konfigurieren | Hinzufügen**.
2. Fügen Sie im Dialogfeld **Regel für automatisches Hinzufügen konfigurieren** die benötigten Daten zum Definieren der Regel hinzu, und klicken Sie dann auf **OK**.

Die neue Regel wird zur Liste der Regel für automatisches Hinzufügen im Dialogfeld **Editor für automatisch hinzugefügte Regeln** hinzugefügt. Dann können Sie die Regel auswählen, damit Datenquellen erstellt werden, wenn automatisch erlernte Daten den in der Regel definierten Kriterien entsprechen.

Festlegen des Datumsformats für Datenquellen

Wählen Sie das Format für in Datenquellen enthaltene Datumsangaben aus.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur einen Empfänger aus, und klicken Sie dann auf das Symbol **Datenquelle hinzufügen**  .
2. Klicken Sie auf **Erweitert**, und treffen Sie dann im Feld **Datumsreihenfolge** eine Auswahl:
   - **Standard**: Verwendet die standardmäßige Datumsreihenfolge (Monat vor Tag). Bei der Verwendung von Client-Datenquellen erben Clients, die diese Einstellung verwenden, die Datumsreihenfolge der übergeordneten Datenquelle.
   - **Monat vor Tag**: Der Monat ist vor dem Tag angegeben (04.23.2014).
   - **Tag vor Monat**: Der Tag ist vor dem Monat angegeben (23.04.2014).
3. Klicken Sie auf **OK**.

Nicht synchronisierte Datenquellen

Aufgrund verschiedener möglicher Einstellungen kann es dazu kommen, dass die Uhrzeit einer Datenquelle nicht mehr mit ESM synchronisiert ist. Wenn durch eine nicht synchronisierte Datenquelle

ein Ereignis generiert wird, wird in der Systemnavigationsstruktur neben dem Empfänger eine rote Kennzeichnung angezeigt.

Sie können einen Alarm einrichten, damit Sie in diesem Fall benachrichtigt werden. Dann können Sie die nicht synchronisierten Datenquellen verwalten, indem Sie auf die Seite **Zeitdelta** zugreifen (siehe *Verwalten nicht synchronisierter Datenquellen*).

Bei nicht synchronisierten Ereignissen kann es sich um alte oder um zukünftige Ereignisse handeln.

Es gibt verschiedene Gründe, aus denen Datenquellen nicht mit ESM synchronisiert sind.

1. Die Zeitzoneneinstellung in ESM ist falsch (siehe *Auswählen von Benutzereinstellungen*).
2. Sie haben beim Hinzufügen der Datenquelle eine falsche Zeitzone festgelegt (siehe *Hinzufügen einer Datenquelle*).
3. Das System ist seit langer Zeit in Betrieb, und die Uhrzeit hat sich im Lauf der Zeit verschoben und ist jetzt nicht mehr synchronisiert.
4. Sie haben das System bewusst so eingerichtet.
5. Das System ist nicht mit dem Internet verbunden.
6. Das Ereignis ist beim Eingang auf dem Empfänger nicht synchronisiert.

Siehe auch

Hinzufügen einer Datenquelle auf Seite 74
Verwalten nicht synchronisierter Datenquellen auf Seite 81
Auswählen von Benutzereinstellungen auf Seite 30

Verwalten nicht synchronisierter Datenquellen

Wenn Sie Datenquellen haben, die nicht mit ESM synchronisiert sind, können Sie einen Alarm einrichten, damit Sie benachrichtigt werden, wenn durch diese Datenquellen Ereignisse generiert werden. Dann können Sie eine Liste der Datenquellen anzeigen, ihre Einstellungen bearbeiten und die Liste exportieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Richten Sie einen Alarm ein, damit Sie benachrichtigt werden, wenn beim Empfänger ein Ereignis eingeht, das durch eine nicht mit ESM synchronisierte Datenquelle generiert wurde.
   a. Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften** .
   b. Klicken Sie auf **Alarme** | **Hinzufügen**, geben Sie auf der Registerkarte **Übersicht** die erforderlichen Informationen ein, und klicken Sie dann auf die Registerkarte **Bedingung**.
   c. Wählen Sie im Feld **Typ** die Option **Ereignisdelta** aus, wählen Sie aus, wie oft von ESM eine Überprüfung auf nicht synchronisierte Datenquellen vorgenommen werden soll. Wählen Sie den Zeitunterschied aus, der erforderlich ist, damit der Alarm ausgelöst wird.
   d. Geben Sie die Informationen auf den verbleibenden Registerkarten ein.
2. Sie können nicht synchronisierte Datenquellen anzeigen, bearbeiten oder exportieren.
   a. Klicken Sie in der Systemnavigationsstruktur auf den Empfänger und dann auf das Symbol **Eigenschaften**.
   b. Klicken Sie auf **Empfängerverwaltung** und dann auf **Zeitdelta**.

Hinzufügen einer untergeordneten Datenquelle

Sie können untergeordnete Datenquellen hinzufügen, damit Sie die Datenquellen besser anordnen können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquellen**.
2. Klicken Sie in der Tabelle der Datenquellen auf die Datenquelle, zu der Sie eine untergeordnete Datenquelle hinzufügen möchten.
3. Klicken Sie auf **Untergeordnetes Element hinzufügen**, und füllen Sie dann die Felder wie bei einer übergeordneten Datenquelle aus.
4. Klicken Sie auf **OK**.

Die Datenquelle wird in der Tabelle und in der Systemnavigationsstruktur unter der übergeordneten Datenquelle als untergeordnetes Element hinzugefügt.

Client-Datenquellen

Sie können die Anzahl der zulässigen Datenquellen auf einem Empfänger erhöhen, indem Sie Client-Datenquellen hinzufügen. Für Datenquellen mit Syslog-, ASP-, CEF-, MEF-, NPP- und WMI-Erfassung können Sie bis zu 65.534 Datenquellen-Clients hinzufügen.

Wenn es sich bereits um eine übergeordnete oder untergeordnete Datenquelle oder um eine WMI-Datenquelle handelt und **RPC verwenden** ausgewählt ist, steht diese Option nicht zur Verfügung.

Sie können mehrere Client-Datenquellen mit der gleichen IP-Adresse verwenden und die Datenquellen anhand der Portnummer unterscheiden. Auf diese Weise können Sie die Daten trennen, indem Sie für die einzelnen Datentypen unterschiedliche Ports verwenden und dann die Daten über den gleichen Port weiterleiten, an dem sie eingegangen sind.

Beim Hinzufügen einer Client-Datenquelle (siehe *Client-Datenquellen* und *Hinzufügen einer Client-Datenquelle*) wählen Sie aus, ob der Port der übergeordneten Datenquelle oder ein anderer Port verwendet werden soll.

Client-Datenquellen haben die folgenden Merkmale:

- Sie haben keine VIPS-Rechte, Richtlinienrechte oder Agenten-Rechte.
- Sie werden in der Tabelle **Datenquellen** nicht angezeigt.
- Sie werden in der Systemnavigationsstruktur angezeigt.

- Für sie gelten die gleichen Richtlinien und Rechte wie für die übergeordnete Datenquelle.
- Sie müssen sich in der gleichen Zeitzone befinden, da für sie die Konfiguration der übergeordneten Datenquelle verwendet wird.



Für Client-WMI-Datenquellen können unabhängige Zeitzonen festgelegt sein, da die Zeitzone durch die an den WMI-Server gesendete Abfrage bestimmt wird.

Hinzufügen einer Client-Datenquelle

Fügen Sie einen Client zu einer vorhandenen Datenquelle hinzu, um die Anzahl der auf dem Empfänger zulässigen Datenquellen zu erhöhen.

Bevor Sie beginnen

Fügen Sie die Datenquelle zum Empfänger hinzu (siehe *Hinzufügen einer Datenquelle*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquellen**.
2. Wählen Sie die Datenquelle aus, zu der Sie den Client hinzufügen möchten, und klicken Sie dann auf **Clients**.

   Auf der Seite **Datenquellen-Clients** werden die Clients aufgeführt, die zurzeit Bestandteil der ausgewählten Datenquelle sind.
3. Klicken Sie auf **Hinzufügen**, geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Ereignisse werden an die spezifischere Datenquelle (übergeordnete Datenquelle oder Client) geleitet. Beispiel: Sie haben zwei Client-Datenquellen, eine mit der IP-Adresse 1.1.1.1 und eine zweite mit der IP-Adresse 1.1.1.0/24, die einen Bereich abdeckt. Beide weisen den gleichen Typ auf. Wenn ein Ereignis mit 1.1.1.1 übereinstimmt, wird es an den ersten Client geleitet, da es spezifischer ist.

Suchen nach einem Client

Auf der Seite **Datenquellen-Clients** werden alle im System vorhandenen Clients aufgeführt. Da mehr als 65.000 Clients vorhanden sein können, wird eine Suchfunktion bereitgestellt, damit Sie bei Bedarf einen bestimmten Client finden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquellen** | **Clients**.
2. Geben Sie die gesuchten Informationen ein, und klicken Sie dann auf **Suchen**.

Importieren einer Liste von Datenquellen

Mit der Option **Importieren** auf der Seite **Datenquellen** können Sie eine Liste von Datenquellen im CSV-Format importieren. Dadurch entfällt das Hinzufügen, Bearbeiten oder Entfernen der einzelnen Datenquellen.

Diese Option verwenden Sie in zwei Situationen:

- Sie möchten unbearbeitete Datenquellendaten von einem Empfänger an einem sicheren Speicherort auf einem Empfänger an einem unsicheren Speicherort importieren. Weitere Informationen hierzu finden Sie unter *Verschieben von Datenquellen auf ein anderes System*.
- Sie möchten die Datenquellen auf einem Empfänger bearbeiten, indem Sie Datenquellen zur vorhandenen Liste hinzufügen, vorhandene Datenquellen bearbeiten oder vorhandene Datenquellen entfernen. Führen Sie in diesem Fall die folgenden Schritte aus.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Exportieren Sie eine Liste der zurzeit auf dem Empfänger vorhandenen Datenquellen.

a Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquellen**.

b Klicken Sie auf **Exportieren** und dann auf **Ja**, um den Download zu bestätigen.

c Wählen Sie den Speicherort für den Download aus, ändern Sie gegebenenfalls den Dateinamen, und klicken Sie dann auf **Speichern**.

Die Liste der vorhandenen Datenquellen wird gespeichert.

d Greifen Sie auf die Datei zu, und öffnen Sie sie.

Daraufhin wird eine Tabelle mit den Daten für die zurzeit auf dem Empfänger vorhandenen Datenquellen geöffnet (siehe *Tabellenfelder für das Importieren von Datenquellen*).

2 Sie können Datenquellen in der Liste hinzufügen, bearbeiten oder entfernen.

a Legen Sie in Spalte A die Aktion fest, die für die Datenquelle ausgeführt werden soll: Hinzufügen, Bearbeiten oder Entfernen.

b Wenn Sie Datenquellen hinzufügen oder bearbeiten, geben Sie die Informationen in die Tabellenspalten ein.

Die Richtlinie oder den Namen der Datenquelle können Sie nicht bearbeiten.

c Sprechen Sie die in der Tabelle vorgenommenen Änderungen.

Sie können nicht eine Datenquelle bearbeiten, um sie als Datenquelle von einer Client-Datenquelle oder umgekehrt festzulegen.

3 Importieren Sie die Liste auf dem Empfänger.

a Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquellen**.

b Klicken Sie auf **Importieren**, wählen Sie die Datei aus, und klicken Sie auf **Hochladen**.

Die Richtlinie oder den Namen der Datenquelle können Sie nicht ändern.

Die Seite **Datenquellen importieren** wird geöffnet. Hier werden die an der Tabelle vorgenommenen Änderungen aufgeführt.

c Zum Importieren der Änderungen klicken Sie auf **OK**.

Die richtig formatierten Änderungen werden hinzugefügt.

d Wenn die Formatierung der Änderungen Fehler enthält, werden diese in einem **Nachrichtenprotokoll** beschrieben.

e Klicken Sie auf **Gesamte Datei herunterladen** und dann auf **Ja**.

f Wählen Sie den Speicherort für den Download aus, ändern Sie bei Bedarf den Namen der Datei, und klicken Sie dann auf **Speichern**.

g Öffnen Sie die heruntergeladene Datei.

Sie enthält eine Liste der Datenquellen, bei denen Fehler aufgetreten sind.

h Korrigieren Sie die Fehler, speichern Sie die Datei, und schließen Sie sie.

i Schließen Sie **Nachrichtenprotokoll** und **Datenquellen importieren**, klicken Sie dann auf **Importieren**, und wählen Sie die gespeicherte Datei aus.

Unter **Datenquellen importieren** werden die korrigierten Datenquellen aufgeführt.

j Klicken Sie auf **OK**.

Tabellenfelder für das Importieren von Datenquellen

Die Tabelle, die Sie zum Importieren von Datenquellen verwenden, enthält mehrere Spalten. Einige sind erforderlich, und andere werden nur für bestimmte Datenquellentypen verwendet.

Für alle Datenquellen erforderliche Felder

Spalte	Beschreibung	Details
op	Für die Datenquelle auszuführender Vorgang	Geben Sie in die Spalte **op** eine dieser Funktionen ein: • **add** = Datenquelle hinzufügen • **edit** = Vorhandene Datenquelle ändern • **remove** = Ohne Neuzuweisung entfernen Wenn diese Spalte leer bleibt, wird keine Aktion für die Datenquelle ausgeführt.
rec_id	Empfänger-ID	Diese Geräte-ID finden Sie auf der Seite **Name und Beschreibung** des Empfängers.
dsname	Name für die Datenquelle	Muss auf dem Empfänger eindeutig sein.

Von allen Datenquellen verwendete Felder

Spalte	Beschreibung	Details
ip	Gültige IP-Adresse für die Datenquelle	• Erforderlich. Ausnahme: Protokoll = 'corr' • Die Überprüfung wird nur für aktivierte Datenquellen ausgeführt. Ausgeschlossen: • Protokolle: cifs, nfs, ftp, scp, http • Collector = 'curl' oder 'mount' • SNMPTrap: Nicht gültig, wenn für andere Datenquellen SNMP-Trap und IPAddress-Übereinstimmungen verwendet werden. • nfxsql: Nicht gültig, wenn eine Kombination aus IPAddress, 'dbname' und 'port' gefunden wird. • netflow oder opsec: Nicht gültig, wenn eine Kombination aus IPAddress und 'port' gefunden wird. • mef: Entspricht der Erfassung (wenn parser mef entspricht, collector wird automatisch auf mef festgelegt). Nicht gültig, wenn mef und protocol gefunden werden.
model		Eintrag muss genau übereinstimmen. Ausnahme: Clients mit MatchByFlag = 1 (Vergleich nach IPAddress)
vendor		Eintrag muss genau übereinstimmen. Ausnahme: Clients mit MatchByFlag = 1 (Vergleich nach IPAddress)
parent_id	ID der übergeordneten Datenquelle	Für Agenten oder Clients erforderlich. Wenn es sich bei der ID um einen Namen handelt, wird versucht, die übergeordnete Datenquelle mit diesem Namen zu finden, die dem angegebenen Empfänger untergeordnet ist.
child_type	Typ der untergeordneten Datenquelle	Erforderlich: 0 = nicht untergeordnet, 1 = Agent, 2 = Client
match_type	Client-Übereinstimmung	Erforderlich beim Hinzufügen oder Bearbeiten von Datenquellen: 1 = Vergleich nach IP-Adresse, 2 = Vergleich nach Typ des Drittanbieters
parsing	Kennzeichnung für aktivierte Datenquelle	Kennzeichnung für Aktivierung (yes/no), Standardwert: yes

Von Datenquellen, die nicht Clients sind, verwendete Felder

Spalte	Beschreibung	Details
snmp_trap_id	Profil-ID für SNMP-Trap	Standardwert: `0`
elm_logging	In ELM protokollieren (yes/no)	Standardwert: `no`
pool	ELM-Poolname	Standardwert: leer
meta-vendor		Standardwert: leer
meta-product		Standardwert: leer
meta_version		Standardwert: leer
url	URL für Ereignisdetails	Standardwert: leer

Spalte	Beschreibung	Details
parser	Analysemethode für das Datenformat	Standardwert: **Default**
collector	Methode für den Datenabruf	Standardwert: **Default** Wenn **parser** **mef** entspricht, wird **collector** auf **mef** festgelegt. scp, http, ftp, nfs, cifs können verwendet werden, wenn das Flatfile-Format für das Protokoll unterstützt wird.

Erforderliche Felder für das Format CEF oder MEF

Spalte	Beschreibung	Details
encrypt	Kennzeichnung für Verschlüsselung der Datenquelle	Standardwert: **F** Wird auch verwendet, wenn **Format** auf **Default**, **Retrieval** auf **mef** und **Protocol** auf **gsyslog** festgelegt ist. Die Verschlüsselung muss für alle MEF-Datenquellen mit der gleichen IP-Adresse gleich sein.
hostname	Hostname oder Host-ID	Standardwert: leer. Optional, wenn **Protocol** auf **gsyslog** oder **syslog** festgelegt ist. Muss eindeutig sein. Optional, wenn **Protocol** auf **nas** festgelegt ist.
aggregate	Syslog-Relay	Gültige Werte: leer und **syslogng**. Standardwert: leer. Wird auch verwendet, wenn **Format** auf **Default**, **Retrieval** auf **Default** und **Protocol** auf **gsyslog** festgelegt ist.
tz_id	ID der Zeitzone	Standardwert: leer Wird auch verwendet, wenn **Format** auf **Default** festgelegt ist und eine der folgenden Bedingungen zutrifft: • **Protocol** ist **syslog**, und **Model** ist nicht **Adiscon Windows Events**. • **Protocol** ist **nfxsql**. • **Protocol** ist **nfxhttp**. • **Protocol** ist **email**. • **Protocol** ist **estream**. Wird auch in gewissem Umfang für die Unterstützung von Flatfiles verwendet.

Sonstige Felder

Spalte	Beschreibung	Details
profile_id	Der Profilname oder die ID	Standardwert: leer. Wenn der Profildatensatz nicht anhand des Profilnamens gefunden wurde, wird ein Fehler protokolliert.
exportMcAfeeFile	Kennzeichnung für Transport der Datenquelle	Standardwert: no. Wenn yes festgelegt ist, wird diese Datenquelle in den Transport der Datenquelle eingeschlossen.
exportProfileID	Der Name des Remote-Freigabeprofils	Standardwert: leer.
mcafee_formated_file	Kennzeichnung für Rohdatendatei analysieren	Standardwert: no. Wenn yes festgelegt ist, wird die Rohdatendatei von der Analysemethode verwendet.
mcafee_formated_file_xsum	Kennzeichnung für Prüfsumme verwenden	Standardwert: no. Wenn yes festgelegt ist, wird die Prüfsumme verwendet, bevor die Rohdatendatei analysiert wird.

Spalte	Beschreibung	Details
mcafee_formated_file_ipsid	Die ursprüngliche Nitro IPS-ID.	Erforderlich bei Verwendung der Rohdatendatei.
zoneID	Name der Zone	Standardwert: leer.
policy_name	ID oder Name der Richtlinie	Standardwert: leer. Wird nur beim Hinzufügen neuer Datenquellen verwendet. Beim Bearbeiten wird dieser Wert nicht aktualisiert.

Für festgelegte Protokolle überprüfte Felder

Das Protokoll wird durch Anbieter und Modell bestimmt. Ausnahme: Wenn das Format auf **Default** oder **CEF** festgelegt ist und **Retrieval** nicht **Default** oder **MEF** entspricht. Dann entspricht das Protokoll dem Wert von **Retrieval**. Wenn kein Profil festgelegt ist, werden diese Felder für das festgelegte Protokoll überprüft.

Tabelle 3-2 Netflow-Felder ab Spalte AF

Spalte	Beschreibung	Details
netflow_port		Standardwert: 9993
netflow_repeat_enabled	Weiterleitung aktiviert	Standardwert: F
netflow_repeat_ip	IP-Adresse für Weiterleitung	Erforderlich, wenn repeat_enabled = T. Standardwert: leer.
netflow_repeat_port	Weiterleitungs-Port	Standardwert: 9996

Tabelle 3-3 rdep-Felder ab Spalte AJ

Spalte	Beschreibung	Details
rdep_sdee_username		Erforderlich
rdep_sdee_password		Erforderlich
rdep_sdee_interval		Standardwert: 60 Sekunden

Tabelle 3-4 opsec-Felder ab Spalte AM

Spalte	Beschreibung	Details
opsec_parent	Kennzeichnung für übergeordnete Elemente (Gerätetyp)	Erforderlich (T/F). T = Datenquelle ist übergeordnet. F = Datenquelle ist nicht übergeordnet.
opsec_authentication	Kennzeichnung für Authentifizierung verwenden	Wird verwendet, wenn übergeordnetes Element = T. Standardwert: F
opsec_appname	Anwendungsname	Erforderlich, wenn authentication = T, optional wenn F, Standardwert: leer
opsec_actkey	Aktivierungsschlüssel	Erforderlich, wenn authentication = T, optional wenn F, Standardwert: leer
opsec_parent_id	Name der übergeordneten Datenquelle	Name des übergeordneten Elements. Erforderlich, wenn übergeordnetes Element = F. Wenn die übergeordnete Datenquelle nicht anhand des Namens der übergeordneten Datenquelle gefunden wurde, wird ein Fehler protokolliert.
opsec_port		Wird verwendet, wenn übergeordnetes Element = T. Standardwert: 18184

Tabelle 3-4 opsec-Felder ab Spalte AM *(Fortsetzung)*

Spalte	Beschreibung	Details
opsec_encryption	Kennzeichnung für Verschlüsselung verwenden	Wird verwendet, wenn übergeordnetes Element = T. Standardwert: F
opsec_comm_method	Kommunikationsmethode	Wird verwendet, wenn übergeordnetes Element = T. Standardwert: leer Muss ein gültiger Wert sein: • '' (leer) • 'asym_sslca' • 'asym_sslca _comp' • 'asym_sslca _rc4' • 'asym_sslca _rc4_comp' • 'ssl_clear' • 'sslca' • 'sslca_clear', • 'sslca_comp' • 'sslca_rc4' • 'sslca_rc4_c omp'
opsec_server_entity_dn	Eindeutiger Name der Server-Entität	Standardwert: leer. Wird verwendet, wenn übergeordnetes Element = T. Erforderlich, wenn DeviceType = Log Server/CLM oder Secondary SMS/CMA.
opsec_collect_audit_events	OPSEC-Ereigniserfassungstyp für Audit-Ereignisse	Wird verwendet, wenn übergeordnetes Element = T. Standardwert: "yes"
opsec_collect_log_events	Kennzeichnung für OPSEC-Ereigniserfassungstyp für Protokollereignisse	Wird verwendet, wenn übergeordnetes Element = T. Standardwert: "yes"
opsec_type	Gerätetyp	Erforderlich. Gültige Werte für dieses Feld: **Wert** / **Name in der Dropdown-Liste für Thin Client** 0 SMS/CMA 1 Security Device 2 Log Server/CLM 3 Secondary SMS/CMA

Tabelle 3-5 wmi-Felder ab Spalte AY

Spalte	Beschreibung	Details
wmi_use_rpc	Kennzeichnung für RPC verwenden	Standardwert: **no**
wmi_logs	Ereignisprotokolle	Standardwert: **SYSTEM,APPLICATION,SECURITY**
wmi_nbname	NetBIOS-Name	Erforderlich, wenn **Retrieval** = **Default**, anderenfalls optional. Standardwert: leer
wmi_username	Benutzername	Erforderlich, wenn **Retrieval** = **Default**, anderenfalls optional. Standardwert: leer
wmi_password	Kennwort	Erforderlich, wenn **Retrieval** = **Default**, anderenfalls optional. Standardwert: leer

Tabelle 3-5 wmi-Felder ab Spalte AY *(Fortsetzung)*

Spalte	Beschreibung	Details
wmi_interval		Standardwert: **600**
wmi_version		Standardwert: **0**

Tabelle 3-6 gsyslog-Felder ab Spalte BF

Spalte	Beschreibung	Details
gsyslog_autolearn	Kennzeichnung für Generische Syslogs unterstützen	Gültige Werte: **T**, **F**, **COUNT**. Standardwert: **F**
gsyslog_type	Zuweisung generischer Regeln	Erforderlich, wenn **autolearn** = **T**, anderenfalls optional. Standardwert: **49190**
gsyslog_mask		Wird verwendet, wenn **Retrieval** auf **Default** festgelegt ist. Standardwert: **0**

Tabelle 3-7 corr-Feld – Spalte BI

Spalte	Beschreibung	Details
corr_local	Kennzeichnung für Lokale Daten verwenden	Standardwert: **F** Bei den Empfängermodellen ERC-VM-25 und ERC-VM-500 wird die Datenquelle nicht hinzugefügt. Anderenfalls kann das Protokoll nicht von anderen Datenquellen verwendet werden.

Tabelle 3-8 sdee-Felder ab Spalte BJ

Spalte	Beschreibung	Details
sdee_username		Erforderlich
sdee_password		Erforderlich
sdee_uri		Standardwert: **cgi-bin/sdee-server**
sdee_interval		Standardwert: **600 Sekunden**
sdee_port		Standardwert: **443**
sdee_proxy_port		Standardwert: **8080**
sdee_use_ssl		Standardwert: **T**
sdee_proxy_ip		Erforderlich, wenn **use_proxy** = **T**. Standardwert: leer
sdee_proxy_username		Erforderlich, wenn **use_proxy** = **T**. Standardwert: leer
sdee_proxy_password		Erforderlich, wenn **use_proxy** = **T**. Standardwert: leer
sdee_use_proxy		Standardwert: **F**

Tabelle 3-9 mssql-Felder ab Spalte BU

Spalte	Beschreibung	Details
mssql_parent	Geräte-Typ	Standardwert: **T Server** = **T. Verwaltetes Gerät** = **F**
mssql_port		Wird verwendet, wenn übergeordnetes Element = **T**. Standardwert: **1433**
mssql_interval		Wird verwendet, wenn übergeordnetes Element = **T**. Standardwert: **600 Sekunden**
mssql_username		Erforderlich, wenn übergeordnetes Element = **T**. Standardwert: leer

Tabelle 3-9 mssql-Felder ab Spalte BU *(Fortsetzung)*

Spalte	Beschreibung	Details
mssql_password		Erforderlich, wenn übergeordnetes Element = **T**. Standardwert: leer
mssql_parent_id	Name des übergeordneten Elements	Erforderlich, wenn übergeordnetes Element = **F**. Wenn die Datenquelle nicht anhand des Namens des übergeordneten Elements gefunden wurde, wird ein Fehler protokolliert.

Tabelle 3-10 syslog-Felder ab Spalte CA

Spalte	Beschreibung	Details
syslog_untrust_iface	Schnittstelle mit niedrigster Vertrauenswürdigkeit	Erforderlich, wenn der **Vendor** auf **CyberGuard** festgelegt ist.
syslog_burb	Name des Internet-Bereichs	Erforderlich, wenn **Vendor** auf McAfee und **Model** auf McAfee Firewall Enterprise festgelegt ist.
syslog_sg_mc	Kennzeichnung für Verwaltungszentrale	Optional, wenn **Vendor** auf Stonesoft Corporation festgelegt ist. Standardwert: no
syslog_nsm	Kennzeichnung für Security Manager	Optional, wenn **Vendor** auf Juniper Networks und Model auf Netscreen Firewall/Security Manager oder Netscreen IDP festgelegt ist. Standardwert: no
syslog_wmi_syslog_format		Optional, wenn **Vendor** auf Microsoft und Model auf Adiscon Windows Events festgelegt ist. Standardwert: 0
syslog_wmi_version		Optional, wenn **Vendor** auf Microsoft und Model auf Adiscon Windows Events festgelegt ist. Standardwert: Windows 2000
syslog_aruba_version		Optional, wenn **Vendor** auf Aruba festgelegt ist. Standardwert: 332
syslog_rev_pix_dir	Netzwerkwerte umkehren	Optional, wenn **Vendor** auf Cisco und Model auf PIX/ASA oder Firewall Services Module festgelegt ist. Standardwert: no
syslog_aggregate	Syslog-Relay	Gültige Werte: leer und **Vendor**. Standardwert: leer
syslog_require_tls	T/F	Gibt an, ob TLS für diese Datenquelle verwendet wird.
syslog_syslog_tls_port		Der Port, der für Syslog TLS verwendet werden soll, wenn dies verwendet wird.
syslog_mask	Maske für IP-Adresse	(Optional) Ermöglicht das Anwenden einer Maske auf eine IP-Adresse, damit ein Bereich von IP-Adressen akzeptiert werden kann. Eine Null (**0**) im Feld bedeutet, dass keine Maske verwendet wird. Standardwert: **0**

Tabelle 3-11 nfxsql-Felder ab Spalte CM

<table>
<tr><th>Spalte</th><th>Beschreibung</th><th>Details</th></tr>
<tr><td>nfxsql_port</td><td></td><td>Der Standard hängt vom Anbieter und Modell ab:
Standardwert | Anbieter | Modell
9117 | Enterasys Networks | Dragon Sensor oder Dragon Squire
1433 | IBM | ISS Real Secure Desktop Protector oder ISS Real Secure Network oder ISS Real Secure Server Sensor
1433 | McAfee | ePolicy Orchestrator oder ePolicy Orchestrator Firewall oder ePolicy Orchestrator Host IPS
3306 | Symantec | Symantec Mail Security for SMTP
1433 | Websense | Websense Enterprise
1433 | Microsoft | Operations Manager
1433 | NetIQ | NetIQ Security Manager
1433 | Trend Micro | Control Manager
1433 | Zone Labs | Integrity Server
1433 | Cisco | Security Agent
1127 | Sophos | Sophos Antivirus
1433 | Symantec | Symantec Antivirus Corporate Edition Server
443 | alle anderen</td></tr>
<tr><td>nfxsql_userid</td><td></td><td>Erforderlich</td></tr>
<tr><td>nfxsql_password</td><td></td><td>Erforderlich</td></tr>
<tr><td>nfxsql_dbname</td><td>Datenbankname</td><td>(Optional) Standardwert: leer</td></tr>
<tr><td>nfxsql_splevel</td><td>Service Pack-Ebene</td><td>Wird verwendet, wenn Vendor auf IBM und Model auf ISS Real Secure Desktop Protector, ISS Real Secure Network oder ISS Real Secure Server Sensor festgelegt ist. Standardwert: SP4</td></tr>
<tr><td>nfxsql_version</td><td></td><td>(Optional)
• Der Standardwert ist 9i, wenn Vendor auf Oracle und Model auf Oracle Audits festgelegt ist.
• Der Standard ist 3.6, wenn Vendor auf McAfee und Model auf ePolicy Orchestrator oder ePolicy Orchestrator Firewall oder ePolicy Orchestrator Host IPS festgelegt ist.</td></tr>
<tr><td>nfxsql_logtype</td><td>Protokollierungstyp</td><td>Erforderlich, wenn Vendor auf Oracle und Model auf Oracle Audits (FGA, GA oder beide) festgelegt ist.</td></tr>
<tr><td>nfxsql_sid</td><td>Datenbank-SID</td><td>Optional, wenn Vendor auf Oracle und Model auf Oracle Audits festgelegt ist. Standardwert: leer</td></tr>
</table>

Tabelle 3-12 nfxhttp-Felder ab Spalte CU

Spalte	Beschreibung	Details
nfxhttp_port		Standardwert: **433**
nfxhttp_userid		Erforderlich
nfxhttp_password		Erforderlich
nfxhttp_mode		Standardwert: **secure**

Tabelle 3-13 email-Felder ab Spalte CY

Spalte	Beschreibung	Details
email_port		Standardwert: **993**
email_mailbox	E-Mail-Protokoll	Standardwert: **imap pop3**
email_connection	Verbindungstyp	Standardwert: **ssl clear**
email_interval		Standardwert: **600 Sekunden**
email_userid		Erforderlich
email_password		Erforderlich

Tabelle 3-14 estream-Felder ab Spalte DE

Spalte	Beschreibung	Details
Diese Felder sind in der Tabelle enthalten. Da jedoch eine Zertifizierungsdatei erforderlich ist, werden die Felder zurzeit ignoriert.		
jestream_port		Standardwert: **993**
jestream_password		Erforderlich
jestream_estreamer_cert_file		Erforderlich
jestream_collect_rna		

Tabelle 3-15 file source-Felder ab Spalte DI

Spalte	Beschreibung	Details
Wird für die Protokolle cifs, ftp, http, nfs und scp verwendet.		
fs_record_lines	Anzahl der Zeilen pro Datensatz	Wird verwendet, wenn **flat file support** verwendet wird. Standardwert: **1**
fs_file_check	Intervall	Standardwert: **15 Minuten**
fs_file_completion		Standardwert: **60 Sekunden**
fs_share_path		Standardwert: leer
fs_filename	Platzhalterausdruck	Erforderlich
fs_share_name		Erforderlich, wenn **Protocol** auf **cifs** oder **nfs** festgelegt ist (wird ansonsten nicht verwendet).
fs_username		Wird verwendet, wenn **Protocol** auf **cifs**, **ftp** oder **scp** festgelegt ist. Standardwert: leer
fs_password		Wird verwendet, wenn **Protocol** auf **cifs**, **ftp** oder **scp** festgelegt ist. Standardwert: leer
fs_encryption		Wird verwendet, wenn **Protocol** auf **ftp** oder **http** festgelegt ist. Standardwert: **no** Wird auch verwendet, wenn **flat file support** und **Protocol** auf **ftp** festgelegt sind.

Tabelle 3-15 file source-Felder ab Spalte DI *(Fortsetzung)*

Spalte	Beschreibung	Details
fs_port		Wird verwendet, wenn **Protocol** auf **ftp** festgelegt ist. Standardwert: **990**. Wenn **Protocol** auf **http** festgelegt ist, lautet der Standardwert **443**. Wird auch verwendet, wenn **flat file support** und **Protocol** auf **ftp** festgelegt sind. Standardwert: **80**
fs_verify_cert	SSL-Zertifikat überprüfen	Wird verwendet, wenn **Protocol** auf **ftp** oder **http** festgelegt ist. Standardwert: **no** Wird auch verwendet, wenn **flat file support** und **Protocol** auf **ftp** festgelegt sind.
fs_compression		Wird verwendet, wenn **Protocol** auf **scp** oder **sftp** festgelegt ist. Standardwert: **no**
fs_login_timeout		Wird verwendet, wenn **Protocol** auf **scp** festgelegt ist. Standardwert: **1 Sekunde**
fs_copy_timeout		Wird verwendet, wenn **Protocol** auf **scp** festgelegt ist. Standardwert: **1 Sekunde**
fs_wmi_version		Wird verwendet, wenn **flat file support** und **Vendor** auf **Microsoft** und **Model** auf **Adiscon Windows Events** festgelegt ist. Standardwert: **Windows 2000**
fs_aruba_version		Wird verwendet, wenn **flat file support** und **Vendor** auf **Aruba** festgelegt sind. Standardwert: **332**
fs_rev_pix_dir	Netzwerkwerte umkehren	Wird verwendet, wenn **flat file support** und **Vendor** auf **Cisco** festgelegt sind und **Model** auf **PIX/ASA** oder **Firewall Services Module** festgelegt ist. Standardwert: **no**
fs_untrust_iface	Schnittstelle mit niedrigster Vertrauenswürdigkeit	Erforderlich, wenn **flat file support** und **Vendor** auf **CyberGuard** festgelegt sind.
fs_burb	Name des Internet-Bereichs	Erforderlich, wenn **flat file support** und **Vendor** auf McAfee und **Model** auf [McAfee Firewall Enterprise] festgelegt sind.
fs_nsm	Kennzeichnung für Security Manager	Optional, wenn **flat file support** und **Vendor** auf **Juniper Networks** festgelegt sind und **Model** auf **Netscreen Firewall/ Security Manager** oder **Netscreen IDP** festgelegt ist. Standardwert: **no**
fs_autolearn	Unterstützung für generisches Syslog	Optional, wenn **flat file support** und **Retrieval** auf **gsyslog** festgelegt sind. Gültige Werte: **T**, **F**, **COUNT**. Standardwert: **F**
fs_type	Zuweisung generischer Regeln	Erforderlich, wenn **autolearn** = **T**, anderenfalls optional. Standardwert: **49190**
fs_binary		Standardwert: **no**
fs_protocol		Standardwert: ' **– Wird verwendet, wenn parser auf Default und collector auf nfs File Source festgelegt ist.**
fs_delete_files		

Tabelle 3-16 sql_ms-Felder ab Spalte EH

Spalte	Beschreibung	Details
sql_ms_port		Standardwert: **1433**
sql_ms_userid		Erforderlich
sql_ms_password		Erforderlich
sql_ms_dbname	Datenbankname	

Tabelle 3-17 nas-Feld – Spalte EL

Spalte	Beschreibung	Details
nas_type		Standardwert: **49190** (Benutzerdefiniert 1). Dieses Feld wird nur für McAfee/PluginProtocol-Datenquellen verwendet.

Tabelle 3-18 ipfix-Feld – Spalte EM

Spalte	Beschreibung	Details
ipfix_transport		Erforderlich. Gültige Werte: **TCP** und **UDP**. **TCP** ist der Standardwert.

Tabelle 3-19 snmp-Felder ab Spalte EN

Spalte	Beschreibung	Details
snmp_authpass	Authentifizierungskennwort	In folgenden Fällen erforderlich: • **traptype** = **v3trap** und **secLevel** = **authPriv** oder **authNoPriv** • **traptype** = **v3inform** und **secLevel** = **authPriv** oder **authNoPriv**
snmp_authproto	Authentifizierungsprotokoll	Gültige Werte: **MD5** oder **SHA1**. In folgenden Fällen erforderlich: • **traptype** = **v3trap** und **secLevel** = **authPriv** oder **authNoPriv** • **traptype** = **v3inform** und **secLevel** = **authPriv** oder **authNoPriv other traptypes**. Standardwert: **MD5**
snmp_community	Community-Name	In folgenden Fällen erforderlich: **traptype** = **v1trap**, **v2trap**, **v2inform**
snmp_engineid		In folgenden Fällen erforderlich: **traptype** = **v3trap**
snmp_privpass	Datenschutzkennwort	In folgenden Fällen erforderlich: • **traptype** = **snmpv3trap** und **secLevel** = **authPriv** • **traptype** = **snmpv3inform** und **secLevel** = **authPriv**
snmp_privproto	Datenschutzprotokoll	Gültige Werte: **DES** und **AES**. In folgenden Fällen erforderlich: • **traptype** = **snmpv3trap** und **secLevel** = **authPriv** • **traptype** = **snmpv3inform** und **secLevel** = **authPriv** Andere **traptypes**, Standardwert: **DES**
snmp_seclevel	Sicherheitsstufe	Gültige Werte: **noAuthNoPriv**, **authNoPriv** und **authPriv** In folgenden Fällen erforderlich: **traptype** = **v3trap** oder **v3inform** Andere **traptypes**, Standardwert: **noAutNoPriv**
snmp_traptype		Erforderlich. Gültige Werte: **v1trap**, **v2trap**, **v2inform**, **v3trap** und **v3inform**
snmp_username		In folgenden Fällen erforderlich: **traptype** = **snmpv3** oder **snmpv3inform**
type	Standardregelzuweisung	Erforderlich. Standardwert: **49190**
snmp_version		Automatisch ausgefüllt

Tabelle 3-20 sql_ws ab Spalte EY

Spalte	Beschreibung	Details
sql_ws_port		(Optional) Standardwert hängt vom Anbieter ab. Standardwert für **Websense: 1433**
sql_ws_userid		Erforderlich
sql_ws_password		Erforderlich
sql_ws_dbname		(Optional) Standardwert: leer
sql_ws_db_instance	Name der Datenbankinstanz	Erforderlich

Tabelle 3-21 sql ab Spalte FD

Spalte	Beschreibung	Details
sql_port	Der für die Verbindung mit der Datenbank verwendete Port	
sql_userid	Datenbankbenutzer-ID	
sql_password	Datenbank-Kennwort	
sql_dbinstance	Name der Datenbankinstanz	
sql_config_logging		Gültige Werte: **0** (für die **SQL Server Express-Datenbank**) und **1** (für die **SQL-Datenbank**)
sql_protocol		Wenn der Wert für **sql_config_logging** auf **1** festgelegt ist, lautet dieser Wert **gsql**.
sql_dbname	Datenbankname	

Tabelle 3-22 oracleidm ab Spalte FK

Spalte	Beschreibung	Details
oracleidm_port	Der für die Verbindung mit der Oracle Identity Manager-Datenbank verwendete Port	
oracleidm_userid	Benutzer-ID für die Oracle Identity Manager-Datenbank	
oracleidm_password	Kennwort für die Oracle Identity Manager-Datenbank	
oracleidm_ip_address	IP-Adresse für die Oracle Identity Manager-Datenbank	
oracleidm_dpsid	TNS-Name der verwendeten Verbindung	

Tabelle 3-23 text ab Spalte FP

Spalte	Beschreibung	Details
	Für die ePolicy Orchestrator-Datenquelle verwendete Felder	
text_dbinstance	Datenbankinstanz, in der die ePolicy Orchestrator-Datenbank ausgeführt wird.	
text_dbname	Name der ePolicy Orchestrator-Datenbank	
text_password	Kennwort für die ePolicy Orchestrator-Datenbank	
text_port	Der für die Verbindung mit der ePolicy Orchestrator-Datenbank verwendete Port	
text_userid	Benutzer-ID für die ePolicy Orchestrator-Datenbank	

Tabelle 3-24 gsql ab Spalte FU

Spalte	Beschreibung	Details
gsql_port		(Optional) Standardwert hängt vom Anbieter ab. Standardwert für **Websense**: **1433**
gsql_userid		Erforderlich
gsql_password		Erforderlich
gsql_dbname		(Optional) Standardwert: leer
gsql_db_instance	Name der Datenbankinstanz	Erforderlich
gsql_nsmversion	NSM-Version	Erforderlich. Wenn der Wert leer bleibt, wird standardmäßig Version 6.X verwendet.

Migrieren von Datenquellen zu einem anderen Empfänger

Sie können Datenquellen zwischen Empfängern im gleichen System erneut zuordnen oder erneut verteilen.

Dies kann besonders hilfreich sein, wenn Sie einen neuen Empfänger erwerben und die Datenquellen und die zugehörigen Daten ausgewogen auf die beiden Empfänger verteilen möchten oder wenn Sie einen größeren Ersatzempfänger kaufen und die Datenquellen vom aktuellen Empfänger auf den neuen übertragen möchten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** für den Empfänger mit den Datenquellen aus, und klicken Sie dann auf **Datenquellen**.

2 Wählen Sie die zu migrierenden Datenquellen aus, und klicken Sie dann auf **Migrieren**.

3 Wählen Sie im Feld **Zielempfänger** den neuen Empfänger aus, und klicken Sie dann auf **OK**.

Verschieben von Datenquellen auf ein anderes System

Zum Verschieben von Datenquellen von einem Empfänger auf einen anderen in einem anderen System müssen Sie die zu verschiebenden Datenquellen auswählen und die Datenquellen und ihre Rohdaten an einem Remote-Speicherort speichern. Anschließend importieren Sie sie auf dem anderen Empfänger.

> **Bevor Sie beginnen**
>
> Um diese Funktion zu verwenden, benötigen Sie auf beiden Empfängern Rechte zur Geräteverwaltung.

Verwenden Sie dieses Verfahren, um Datenquellen von einem Empfänger an einem sicheren Speicherort auf einen Empfänger an einem unsicheren Speicherort zu verschieben.

Beim Exportieren von Datenquelleninformationen gelten Einschränkungen:

- Sie können keine Flussdatenquellen transportieren (beispielsweise IPFIX, NetFlow oder sFlow).
- Die Quellereignisse von korrelierten Ereignissen werden nicht angezeigt.
- Wenn Sie die Korrelationsregeln auf dem zweiten Empfänger ändern, werden diese Regeln vom Korrelationsmodul nicht verarbeitet. Beim Transport der Korrelationsdaten werden diese Ereignisse aus der Datei eingefügt.

Aufgabe	Vorgehensweise
Auswählen der Datenquellen und des Remote-Speicherorts	1 Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquelle**. 2 Wählen Sie die Datenquelle aus, und klicken Sie dann auf **Bearbeiten**. 3 Klicken Sie auf **Erweitert**, und wählen Sie dann **Im NitroFile-Format exportieren** aus. Die Daten werden an einen Remote-Speicherort exportiert und mithilfe des Profils konfiguriert. 4 Klicken Sie auf **OK**. Von nun an werden die von dieser Datenquelle generierten Rohdaten an den Speicherort der Remote-Freigabe kopiert.
Erstellen einer Rohdatendatei	1 Greifen Sie auf den Speicherort der Remote-Freigabe zu, in der die Rohdaten gespeichert sind. 2 Speichern Sie die generierten Rohdaten an einem Speicherort, von dem aus Sie die Datei auf den zweiten Empfänger verschieben können (beispielsweise ein Flash-Laufwerk, das Sie an den nicht gesicherten Speicherort mitnehmen können).
Erstellen einer Datei zur Beschreibung der Datenquellen	1 Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquelle** | **Importieren**. 2 Suchen Sie die Datei mit den verschobenen Datenquellen, und klicken Sie auf **Hochladen**. 3 Wählen Sie in der Liste **Remote-Freigabeprofil** den Speicherort der Rohdatendateien aus. Wenn das Profil nicht aufgeführt ist, klicken Sie auf **Remote-Freigabeprofil**, und fügen Sie das Profil hinzu. 4 Klicken Sie auf **OK**. Die Datenquellen werden zum zweiten Empfänger hinzugefügt und greifen über das Remote-Freigabeprofil auf die Rohdaten zu.
Importieren von Rohdaten und Datenquellendateien	1 Greifen Sie in der Systemnavigationsstruktur auf dem zweiten Empfänger auf **Datenquellen** zu, und klicken Sie dann auf **Importieren**. 2 Suchen Sie die Datei mit den verschobenen Datenquellen, und klicken Sie auf **Hochladen**. Auf der Seite **Datenquellen importieren** werden die zu importierenden Datenquellen aufgeführt. 3 Wählen Sie in der Liste **Remote-Freigabeprofil** den Speicherort der Rohdatendateien aus. Wenn das Profil nicht aufgeführt ist, klicken Sie auf **Remote-Freigabeprofil**, und fügen Sie es Profil hinzu (siehe *Konfigurieren von Profilen*). 4 Klicken Sie auf **OK**.

Einrichten von automatischem Lernen für Datenquellen

Richten Sie ESM für das automatische Erlernen von IP-Adressen ein.

> **Bevor Sie beginnen**
> Stellen Sie sicher, dass Ports für Syslog, MEF und Flüsse definiert sind (siehe *Einrichten von Netzwerkschnittstellen*).

Die Firewall auf dem Empfänger wird für den festgelegten Zeitraum geöffnet, damit unbekannte IP-Adressen vom System erlernt werden können. Anschließend können Sie diese als Datenquellen zum System hinzufügen.



Bei einem Upgrade werden die automatisch erlernten Ergebnisse von der Seite **Automatisch lernen** gelöscht. Wenn automatisch erlernte Ergebnisse vorhanden sind, für die Sie vor dem Upgrade keine Aktion ausgeführt haben, müssen Sie nach dem Upgrade das automatische Lernen ausführen, um diese Ergebnisse erneut zu erfassen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Datenquellen** | **Automatisch lernen**.
2. Definieren Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Schließen**.

Anzeigen der von Datenquellen generierten Dateien

Zum Anzeigen der von Datenquellen generierten Dateien müssen Sie auf die Seite **Dateien anzeigen** zugreifen. In ESM-Ansichten werden die Dateien nicht angezeigt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die McAfee-Datenquelle aus.
2. Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Dateien anzeigen**  .
3. Führen Sie einen der folgenden Schritte aus:
   - Geben Sie in das Feld **Filter für Dateinamen** einen Dateinamen ein, um eine bestimmte Datei zu suchen.
   - Ändern Sie die Einstellungen im Feld **Zeitbereich**, um nur die in diesem Zeitraum generierten Dateien anzuzeigen.
   - Klicken Sie auf **Aktualisieren**, um die Dateiliste zu aktualisieren.
   - Wählen Sie in der Liste eine Datei aus, und klicken Sie dann auf **Herunterladen**, um die Datei herunterzuladen.
4. Klicken Sie auf **Abbrechen**, um die Seite zu schließen.

Benutzerdefinierte Datenquellentypen

Diese Tabelle enthält die benutzerdefinierten Typen und die entsprechenden Namen oder Einträge, die im Datenquellen-Editor angezeigt werden.

ID	Gerätemodell	Anbieter	Protokoll	Namenspräfix für Regeln	Regel-Editor-Typ
49190	Benutzerdefiniert 1	Nicht zutreffend	Syslog	UserDefined1_	Generic
49191	Benutzerdefiniert 2	Nicht zutreffend	Syslog	UserDefined2_	Generic

ID	Gerätemodell	Anbieter	Protokoll	Namenspräfix für Regeln	Regel-Editor-Typ
49192	Benutzerdefiniert 3	Nicht zutreffend	Syslog	UserDefined3_	Generic
49193	Benutzerdefiniert 4	Nicht zutreffend	Syslog	UserDefined4_	Generic
49194	Benutzerdefiniert 5	Nicht zutreffend	Syslog	UserDefined5_	Generic
49195	Benutzerdefiniert 6	Nicht zutreffend	Syslog	UserDefined6_	Generic
49196	Benutzerdefiniert 7	Nicht zutreffend	Syslog	UserDefined7_	Generic
49197	Benutzerdefiniert 8	Nicht zutreffend	Syslog	UserDefined8_	Generic
49198	Benutzerdefiniert 9	Nicht zutreffend	Syslog	UserDefined9_	Generic
49199	Benutzerdefiniert 10	Nicht zutreffend	Syslog	UserDefined10_	Generic

Unterstützte Datenquellen

McAfee fügt regelmäßig Unterstützung für neue Datenquellen hinzu. Auf Empfängern sind maximal 2000, 200 oder 50 Datenquellen möglich.

Informationen zum Anzeigen einer Liste der zurzeit unterstützten Datenquellen finden Sie unter https://kc.mcafee.com/corporate/index?page=content&id=PD25060.

Diesen Geräten können 2.000 Datenquellen zugeordnet werden:

- ERC-1225
- ERC-1250
- ERC-2230
- ERC-2250
- ERC-2600
- ERC-3450
- ERC-4245
- ERC-4600
- ENMELM-2250
- ENMELM-4245
- ENMELM-4600
- ENMELM-5205
- ENMELM-5600
- ENMELM-5750
- ENMELM-6000
- ELMERC-2230
- ELMERC-2250
- ELMERC-2600
- ELMERC-4245
- ELMERC-4600
- ESMREC-4245
- ESMREC-5205
- ESMREC-5510

Beim Modell ERC-110 sind nur 50 Datenquellen zulässig, bei allen anderen maximal 200.

Die Datenquellenbereiche sind wie folgt zugeordnet:

- Datenquellentypen: 1 – 48.999
- Benutzerdefinierte Typen: 49.001 – 49.999
- Für McAfee reserviert (beispielsweise Regelsätze): 50.001 – 65.534



Wenn Sie McAfee Firewall Enterprise Event Reporter (ERU) verwenden, sind nur McAfee-Datenquellen verfügbar.

Konfiguration für bestimmte Datenquellen

Manche Datenquellen erfordern mehr Informationen und spezielle Konfigurationseinstellungen.

In den Abschnitten dieses Anhangs finden Sie weitere Details.

- Check Point
- IBM Internet Security Systems SiteProtector
- McAfee ePolicy Orchestrator
- ePolicy Orchestrator 4.0
- NSM-SEIM
- Unterstützung für Syslog-Relay
- Adiscon
- Big Fix
- Common Event Format
- ArcSight
- Security Device Event Exchange
- Erweiterter Syslog-Parser
- WMI-Ereignisprotokoll

WMI-Ereignisprotokoll

Bei WMI handelt es sich um die Microsoft-Implementierung von Web-Based Enterprise Management (WBEM) gemäß der Definition durch die Distributed Management Task Force (DMTF).

Dies ist die primäre Verwaltungstechnologie für Windows-Betriebssysteme, mit deren Hilfe Verwaltungsinformationen gemeinsam von Verwaltungsanwendungen genutzt werden können. WMI ist hilfreich, da Sie die Möglichkeit haben, Verwaltungsdaten von Remote-Computern abzurufen.

WMI ist nicht FIPS-konform. Verwenden Sie diese Funktion nicht, wenn Sie FIPS-Vorschriften einhalten müssen.

WMI-Ereignisprotokolle werden als Datenquelle eingerichtet und über den Empfänger gesendet. Die Ereignisse werden über den Empfänger in einem festgelegten Intervall vom Windows-Server abgerufen und erfasst. Mit der WMI-Erfassung können Ereignisse aus allen Ereignisprotokollen auf dem Windows-Computer erfasst werden. Standardmäßig werden auf dem Empfänger Sicherheits-, Administrations- und Ereignisprotokolle erfasst. Sie können weitere Protokolldateien eingeben, beispielsweise Verzeichnisdienstprotokolle oder Exchange-Protokolle. Die Ereignisprotokolldaten werden in den Paketdaten erfasst und können über die Details der Ereignistabelle angezeigt werden.

Für WMI-Ereignisprotokolle sind die Berechtigungen eines Administrators oder Sicherungs-Operators erforderlich, es sei denn, Sie verwenden Windows 2008 oder 2008 R2, und die Datenquelle und der Benutzer sind richtig eingerichtet (siehe *Einrichten des Abrufs von Windows-Sicherheitsprotokollen*).

Die folgenden zusätzlichen Geräte werden von der WMI-Datenquelle unterstützt:

- McAfee Antivirus
- Windows
- Microsoft ISA Server
- Microsoft Active Directory
- Microsoft SQL Server
- RSA Authentication Manager
- Symantec Antivirus
- Microsoft Exchange

Anweisungen zum Einrichten von Syslog WMI über Adiscon finden Sie unter *Adiscon-Setup*.

Wenn Sie eine WMI-Datenquelle einrichten, lautet der Anbieter **Microsoft** und das Modell **WMI Event Log**.

Einrichten für das Abrufen von Windows-Sicherheitsprotokollen

Wenn Sie Windows 2008 oder 2008 R2 verwenden und die Datenquelle für das WMI-Ereignisprotokoll richtig eingerichtet ist, können Benutzer ohne Administratorberechtigungen Windows-Sicherheitsprotokolle abrufen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Erstellen Sie auf dem System unter Windows 2008 oder 2008 R2, auf dem Sie Ereignisprotokolle lesen möchten, einen neuen Benutzer.
2. Weisen Sie den Benutzer auf dem Windows-System der Gruppe Ereignisprotokollleser zu.
3. Erstellen Sie in McAfee Event Receiver eine neue Datenquelle für das Microsoft WMI-Ereignisprotokoll. Geben Sie dabei die Anmeldeinformationen für den in Schritt 1 erstellten Benutzer ein (siehe *Hinzufügen einer Datenquelle*).
4. Aktivieren Sie das Kontrollkästchen **RPC verwenden**, und klicken Sie dann auf **OK**.

Korrelationsdatenquelle

Mithilfe einer Korrelationsdatenquelle werden Daten analysiert, die von einem ESM-Gerät fließen, verdächtige Muster innerhalb des Datenflusses entdeckt, den Mustern entsprechende Korrelationswarnungen generiert und die Warnungen in die Warnungsdatenbank des Empfängers eingefügt.

Ein verdächtiges Muster wird durch Daten dargestellt, die mithilfe von Richtlinienregeln für die Korrelation interpretiert werden. Diese Regeln können Sie erstellen und ändern. Diese separaten Regeltypen unterscheiden sich von Nitro IPS-Regeln oder Firewall-Regeln und verfügen über Attribute, mit denen ihr Verhalten angegeben wird.

Sie können ähnlich wie beim Konfigurieren von Syslog oder OPSEC nur eine Korrelationsdatenquelle pro Empfänger konfigurieren. Wenn Sie die Korrelationsdatenquelle eines Empfängers konfiguriert haben, können Sie einen Rollout für die Standardrichtlinie der Korrelation ausführen, die Basisregeln in der Standardrichtlinie der Korrelation bearbeiten oder benutzerdefinierte Regeln und Komponenten hinzufügen und anschließend einen Rollout für die Richtlinie ausführen. Sie können die einzelnen Regeln aktivieren oder deaktivieren und die Werte der vom Benutzer definierbaren Parameter für die einzelnen Regeln festlegen. Details zur Korrelationsrichtlinie finden Sie unter *Korrelationsregeln*.

Wenn Sie eine Korrelationsdatenquelle hinzufügen, lautet der Anbieter **McAfee** und das Modell **Korrelationsmodul**.

Wenn die Korrelationsdatenquelle aktiviert ist, werden vom ESM-Gerät Warnungen an das Korrelationsmodul auf dem Empfänger gesendet.

Zuordnung von Schweregraden und Aktionen

Die Parameter für Schweregrade und Aktionen unterscheiden sich geringfügig in der Verwendung. Das Ziel besteht darin, einen Wert aus der Syslog-Nachricht einem Wert zuzuordnen, der sich in das Schema des Systems einfügt.

- severity_map: Der Schweregrad wird als Wert zwischen 1 (niedrigster Schweregrad) und 100 (höchster Schweregrad) angezeigt, der den mit der Regel übereinstimmenden Ereignissen zugewiesen wird. In manchen Fällen wird der Schweregrad auf dem Gerät, von dem die Nachricht gesendet wird, als Zahl von 1 bis 10 oder als Text (hoch, mittel, niedrig) angezeigt. Da in diesen Fällen der Schweregrad nicht aufgezeichnet werden kann, müssen Sie eine Zuordnung erstellen. Im folgenden Beispiel sehen Sie eine Nachricht von McAfee IntruShield, in der der Schweregrad in Textform angezeigt wird.

  ```
  <113>Apr 21 07:16:11 SyslogAlertForwarder: Attack NMAP: XMAS Probe (Medium)\000
  ```

  Die Syntax für eine Regel mit Zuordnung des Schweregrads würde so aussehen (die Schweregradzuordnung ist nur zur Hervorhebung fett formatiert):

  ```
  alert any any any -> any any (msg:"McAfee Traffic"; content:"syslogalertforwarder";
  severity_map:High=99,Medium=55,Low=10; pcre:"(SyslogAlertForwarder)\x3a\s+Attack\s+
  ([^\x27]+)\x27([^\x28]+)\x28"; raw; setparm:application=1; setparm:msg=2;
  setparm:severity=3; adsid:190; rev:1;)
  ```

  severity_map : High=99,Medium=55,Low=10. Damit wird der Text einer Zahl in einem Format zugeordnet, das Sie verwenden können.

  setparm : severity=3. Dies bedeutet, dass die dritte Aufzeichnung auf den Schweregrad festgelegt werden soll. Alle setparm-Modifizierer funktionieren auf diese Weise.

- action_map: Wird wie der Schweregrad verwendet. Die Aktion entspricht der Aktion, die vom Drittanbietergerät ausgeführt wurde. Mithilfe der Aktion soll eine für den Endbenutzer hilfreiche Zuordnung erstellt werden. Hier ist ein Beispiel für eine Nachricht von OpenSSH zu fehlgeschlagenen Anmeldungen.

  ```
  Dec 6 10:27:03 nina sshd[24259]: Failed password for root from 10.0.12.20 port
  49547 ssh2
  ```

  ```
  alert any any any -> any any (msg:"SSH Login Attempt"; content:"sshd";
  action_map:Failed=9,Accepted=8;
  ```

  ```
  pcre:"sshd\x5b\d+\x5d\x3a\s+((Failed|Accepted)\s+password)\s+for\s+((invalid|
  illegal)\s+user\s+)?(\S+)\s+from\s+(\S+)(\s+(\S+)\s+port\s+(\d+))?"; raw;
  setparm:msg=1; setparm:action=2; setparm:username=5; setparm:src_ip=6; adsid:190;
  rev:1;)
  ```

  Die Aktion (`Failed`) ist einer Zahl zugeordnet. Diese Zahl entspricht den verschiedenen Aktionen, die Sie in Ihrem System verwenden können. In der folgenden Liste finden Sie alle Aktionstypen, die Sie verwenden können.

  - 0 = Null
  - 1 = Zulassen
  - 2 = Ablehnen
  - 3 = Verwerfen
  - 4 = Verwerfen im Hintergrund
  - 5 = Warnung
  - 6 = Standard
  - 20 = Anhalten
  - 21 = Hinweis
  - 22 = Vertrauenswürdig
  - 23 = Nicht vertrauenswürdig
  - 24 = False-Positive
  - 25 = Warnung und ablehnen
  - 26 = Warnung und verwerfen

- 7 = Fehler
- 8 = Erfolg
- 9 = Fehlgeschlagen
- 10 = Notfall
- 11 = Kritisch
- 12 = Warnmeldung
- 13 = Information
- 14 = Debug
- 15 = Integrität
- 16 = Hinzufügen
- 17 = Ändern
- 18 = Entfernen
- 19 = Starten
- 27 = Warnung und verwerfen im Hintergrund
- 28 = Neustart
- 29 = Blockieren
- 30 = Säubern
- 31 = Säubern und Fehlschlag
- 32 = Fortfahren
- 33 = Infiziert
- 34 = Verschieben
- 35 = Verschieben und Fehlschlag
- 36 = Quarantäne
- 37 = Quarantäne und Fehlschlag
- 38 = Entfernen und Fehlschlag
- 39 = Abgelehnt

In diesem Beispiel wird `Failed` aus der Syslog-Nachricht der Zahl 9 zugeordnet, die vom System als `Fehlgeschlagen` gemeldet wird.

Die Struktur einer Regel ist wie folgt aufgebaut.

```
Alert any any any -> any any (msg:”Login Attempt”; content:”sshd”; action_map oder
severity_map (bei Bedarf); pcre:”Ihr regulärer Ausdruck”; raw; setparm:Daten-Tag;
adsid:190; rev:1;)
```

Erweiterter Syslog-Parser

Mithilfe des erweiterten Syslog-Parsers (ASP) können Sie Daten aus Syslog-Nachrichten auf der Basis benutzerdefinierter Regeln analysieren. Mit den Regeln weisen Sie ASP an, wie eine bestimmte Nachricht erkannt werden soll und wo in diesem nachrichtenspezifischen Ereignis sich Daten wie beispielsweise Signatur-IDs, IP-Adressen, Ports, Benutzernamen und Aktionen befinden.

Sie können ASP für Syslog-Geräte verwenden, die auf der Seite **Datenquelle hinzufügen** nicht ausdrücklich identifiziert sind, wenn Nachrichten vom quellspezifischen Parser nicht richtig interpretiert werden oder Datenpunkte im Zusammenhang mit empfangenen Ereignissen vollständig interpretiert werden. Außerdem können Sie so optimal komplexe Protokollquellen wie Linux- und UNIX-Server sortieren. Für diese Funktionalität müssen Sie an die Linux- oder UNIX-Umgebung angepasste Regeln schreiben (siehe *Hinzufügen von Regeln zum erweiterten Syslog-Parser*).

Sie können eine ASP-Datenquelle zum Empfänger hinzufügen, indem Sie Syslog als Anbieter auswählen (siehe *Hinzufügen einer Datenquelle*). Folgen Sie anschließend den Anweisungen des Geräteherstellers, um das Syslog-Gerät so zu konfigurieren, dass Syslog-Daten an die IP-Adresse des Empfängers gesendet werden.

Wenn Sie eine ASP-Quelle hinzufügen, müssen Sie eine Richtlinie anwenden, damit Ereignisdaten erfasst werden. Wenn Sie **Unterstützung für generisches Syslog** aktivieren, können Sie eine Richtlinie ohne Regeln anwenden und Ereignisdaten generisch erfassen.



Bei manchen Datenquellen wie beispielsweise Linux- und UNIX-Servern können große Mengen nicht einheitlicher Daten erzeugt werden. Dies führt dazu, dass die Ergebnisse auf dem Empfänger nicht richtig mit aufgetretenen ähnlichen Ereignissen gruppiert werden. Daher wird ein großer Bereich verschiedener Ereignisse angezeigt, obwohl sich in Wirklichkeit einfach das gleiche Ereignis wiederholt. Dennoch werden unterschiedliche Syslog-Daten an den Empfänger gesendet.

Durch Hinzufügen von Regeln zu ASP können Sie den größten Nutzen aus den Ereignisdaten ziehen. Das in ASP verwendete Format hat große Ähnlichkeit mit dem Snort-Format.

```
ACTION Protocol Src_ip Src_port -> Dst_ip Dst_port (keyword: option; keyword:
option;...;)
```



Schließen Sie beim Verketten eines Literalwerts mit einer PCRE-Teilaufzeichnung in Version 9.0.0 und höher die Literale einzeln in Anführungszeichen ein, wenn sie Leerzeichen oder andere Zeichen enthalten. Lassen Sie die Verweise auf die PCRE-Teilaufzeichnung ohne Anführungszeichen.

Regeln werden wie folgt definiert.

Abschnitt	Feld	Beschreibung
Regelkopfzeile		Die Regelkopfzeile enthält die Benachrichtigungsaktion und das Format any any any. Die Regel lautet: `ALERT any any any -> any any`
	Aktion	Gibt an, was mit dem Ereignis geschehen soll, wenn eine Übereinstimmung vorliegt. Die Optionen lauten: • ALERT: Ereignis protokollieren • DROP: Ereignis protokollieren, aber nicht weiterleiten • SDROP: Ereignis nicht protokollieren oder weiterleiten • PASS: Weiterleiten falls definiert, aber nicht protokollieren
	Protokoll	Wenn im Ereignis ein Protokoll definiert ist, wird basierend auf dem Protokoll nach der effektiven Übereinstimmung gefiltert.
	Src/Dst IP	Wenn im Ereignis eine Quell- oder Ziel-IP-Adresse definiert ist, wird basierend auf dieser Adresse nach der effektiven Übereinstimmung gefiltert.
	Src/Dst Port	Wenn im Ereignis ein Quell- oder Ziel-Port definiert ist, wird basierend auf diesem Port nach der effektiven Übereinstimmung gefiltert.
Regeltext		Der Regeltext enthält den größten Teil der Übereinstimmungskriterien. Hier definieren Sie, wie die Daten analysiert und in der ESM-Datenbank protokolliert werden müssen. Die Elemente des Regeltexts werden in Paaren aus Stichwort und Option definiert. Auf manche Stichwörter folgt keine Option.
	msg	(Erforderlich) Die Nachricht, die der Regel zugeordnet werden soll. Dabei handelt es sich um die Zeichenfolge, die in ESM Thin Client zu Berichterstellungszwecken angezeigt wird, sofern sie nicht durch eine mit pcre/setparm entdeckte Nachricht überschrieben wird (siehe unten). Der erste Teil von msg ist der Kategoriename, gefolgt von der eigentlichen Nachricht (msg: "Kategorie der Regelnachricht").

Abschnitt	Feld	Beschreibung
	content	*(Optional, eines oder mehr)* Beim Inhaltsstichwort handelt es sich um einen Qualifizierer ohne Platzhaltertext zum Vorfiltern von Ereignissen, die den Regelsatz passieren. Kann auch Leerzeichen enthalten (beispielsweise content: "Suche 1"; content "etwas anderes")
	procname	Auf vielen UNIX- und Linux-Systemen ist der Prozessname (und die Prozess-ID) Teil eines standardisierten Syslog-Nachrichten-Headers. Mit dem Stichwort procname können Sie Ereignisübereinstimmungen für die Regel filtern. Wird verwendet, um Ereignisübereinstimmungen auszuschließen oder zu filtern, bei denen zwei Prozesse auf einem Linux- oder UNIX-Server diesen oder einen ähnlichen Nachrichtentext aufweisen.
	adsid	Die Datenquellen-ID, die verwendet werden soll. Mit diesem Wert wird die **Standardregelzuweisung** im Datenquellen-Editor überschrieben.
	sid	Signatur-ID der Regel. Dies ist die Übereinstimmungs-ID, die in ESM Thin Client verwendet wird, sofern sie nicht durch eine mit pcre/setparm entdeckte SID überschrieben wird.
	rev	Regelrevision. Wird zum Verfolgen von Änderungen verwendet.
	Schweregrad	Ein Wert zwischen 1 (niedrigster Schweregrad) und 100 (höchster Schweregrad), der Ereignissen zugewiesen wird, die mit der Regel übereinstimmen.
	pcre	Das PCRE-Stichwort wird für den Vergleich eingehender Ereignisse mithilfe eines PCRE-Ausdrucks (Perl Compatible Regular Expression) verwendet. Der PCRE-Ausdruck wird durch Anführungszeichen getrennt, und alle Vorkommen von "/" werden als normales Zeichen behandelt. Inhalte in Klammern sind für das Stichwort setparm reserviert. Das PCRE-Stichwort kann mit den Stichwörtern nocase, nomatch, raw und setparm geändert werden.
	nocase	Bewirkt, dass der PCRE-Inhalt unabhängig von der Groß-/Kleinschreibung verglichen wird.
	nomatch	Kehrt die PCRE-Übereinstimmung um (entspricht !~ in Perl).
	raw	Vergleicht den PCRE-Ausdruck mit der gesamten Syslog-Nachricht einschließlich der Header-Daten (Einrichtung, Daemon, Datum, Host/IP, Prozessname und Prozess-ID). Normalerweise wird der Header bei der PCRE-Übereinstimmung nicht verwendet.
	setparm	Kann mehrmals vorkommen. Jedem Satz von Klammern im PCRE-Ausdruck wird in der Reihenfolge des Vorkommens eine Nummer zugewiesen. Diese Nummern können Daten-Tags zugewiesen werden (Beispiel: setparm:username=1). Damit wird der aufgezeichnete Text aus dem ersten Satz von Klammern dem Daten-Tag für den Benutzernamen zugewiesen. Die erkannten Tags werden unten in der Tabelle aufgeführt.

Tag	Beschreibung
* sid	Mit diesem aufgezeichneten Parameter wird die SID der übereinstimmenden Regel überschrieben.
* msg	Mit diesem aufgezeichneten Parameter wird die Nachricht oder der Name der übereinstimmenden Regel überschrieben.
* action	Dieser aufgezeichnete Parameter gibt an, welche Aktion vom Drittanbietergerät ausgeführt wurde.
* protocol	
* src_ip	Hiermit wird die IP der Syslog-Quelle, das heißt die standardmäßige Quell-IP eines Ereignisses, ersetzt.
* src_port	
* dst_ip	

Tag	Beschreibung
* dst_port	
* src_mac	
* dst_mac	
* dst_mac	
* genid	Hiermit wird die in der Datenbank gespeicherte SID geändert. Wird für nicht von McAfee stammende Snort-Übereinstimmungen in Snort-Präprozessoren verwendet.
* url	Reserviert, wird jedoch noch nicht verwendet.
* src_username	Erster Benutzername/Quellbenutzername
* username	Alternativer Name für src_username.
* dst_username	Zweiter Benutzername/Quellbenutzername
* domain	
* hostname	
* application	
* severity	Muss eine Ganzzahl sein.
* action map	Hiermit können Sie bestimmte Aktionen des Produkts den McAfee-Aktionen zuordnen. Bei der Aktionszuordnung wird die Groß-/Kleinschreibung beachtet. Beispiel: alert any any any -> any any (msg:"OpenSSH Accepted Password"; content:"Accepted password for "; action_map:Accepted=8, Blocked=3; pcre:"(Accepted)\s+password\s+for\s+(\S+)\s+from\s+(\d+\.\d+\.\d+\.\d+)\s +port\s+(\d+)"; setparm:action=1; sid:31; rev:1;)). Weitere Details finden Sie unter *Zuordnung von Schweregraden und Aktionen*.
* severity map	Hiermit können Sie bestimmte Schweregrade des Produkts den McAfee-Schweregraden zuordnen. Wie bei der Aktionszuordnung wird auch bei der Schweregradzuordnung die Groß-/Kleinschreibung beachtet. Beispiel: alert any any any -> any any (msg:"OpenSSH Accepted Password"; content:"Accepted password for "; severity_map:High=99, Low=25, 10=99, 1=25; pcre:"(Accepted) \s+password\s+for\s+(\S+)\s+from\s+(\d+\.\d+\.\d+\.\d+)\s+port\s+(\d+)"; setparm:action=1; sid:31; rev:1;))pri(?:\x3d|\x3a)\s*(?:p\x5f)?([^\x2c]+). Weitere Details finden Sie unter *Zuordnung von Schweregraden und Aktionen*.

Tag	Beschreibung
* var	Dies ist eine andere Möglichkeit für die Verwendung von setparms. Am besten erstellen Sie jedoch einen Wert aus mehreren Aufzeichnungen durch mehrere PCREs. Sie können anstelle eines großen PCREs mit mehreren Aufzeichnungen mehrere PCREs erstellen, mit denen nur ein kleiner Teil Ihrer Zeichenfolge aufgezeichnet wird. Hier ist ein Beispiel für die Erfassung eines Benutzernamens und einer Domäne sowie die Erstellung einer E-Mail-Adresse zum Speichern im Feld objectname. • Syntax = var:field=${PCRE:Capture} • PCRE = Nicht der eigentliche PCRE, sondern seine Nummer. Wenn die Regel zwei PCREs enthält, handelt es sich um PCRE 1 oder 2. • Capture = Nicht die eigentliche Aufzeichnung, sondern die Nummer (erste, zweite oder dritte Erfassung [1,2,3]) • Beispielnachricht: Ein Mann namens Jim arbeitet für McAfee. • PCRE: (Jim).*?(McAfee) • Regel: alert any any any -> any any (msg:"Var User Jim"; content:"Jim"; pcre:"(Jim)"; pcre:"(McAfee)"; var:src_username=${1:1}; var:domain=${2:1}; var:objectname=${1:1}@${2:1}.com raw; classtype:unknown; adsid:190; sev: 25; sid:610061000; rev:1; normID:1209008128; gensys:T;) • Zugeordneter Quellbenutzer: Jim • Zugeordnete Domäne: McAfee • Zugeordneter Objektname: Jim@McAfee.com
* sessionid	Dies ist eine Ganzzahl.
* commandname	Dies ist ein Zeichenfolgenwert.
* objectname	Dies ist ein Zeichenfolgenwert.
* event_action	Dieses Tag wird verwendet, um eine Standardaktion festzulegen. Sie können event_action und action_map nicht in der gleichen Regel verwenden. Sie können beispielsweise bei einem Ereignis für eine erfolgreiche Anmeldung das Tag event_action verwenden und als Standard für die Aktion den Wert success verwenden (Beispiel: event_action:8;).

Tag	Beschreibung
* firsttime_fmt	Wird verwendet, um das erste Auftreten des Ereignisses festzulegen. Weitere Informationen finden Sie in der Liste der Formate.
* lasttime_fmt	Wird verwendet, um das letzte Auftreten des Ereignisses festzulegen. Weitere Informationen finden Sie in der Liste der Formate. Sie können dies mit setparm oder var verwenden (var:firsttime="${1:1}" oder setparm:lasttime="1"). Beispiel: alert any any any -> any any (msg:"SSH Login Attempt"; content:"content"; firsttime_fmt:"%Y-%m-%dT%H:%M:%S.%f"; lasttime_fmt:"%Y-%m-%dT%H:%M:%S.%f" pcre:"PCRE goes here; raw; setparm:firsttime=1; setparm:lasttime=1; adsid:190; rev:1;) Weitere Details zu unterstützten aktuellen Formaten finden Sie unter http://pubs.opengroup.org/onlinepubs/009695399/functions/strptime.html. %Y - %d - %m %H : %M : %S %m - %d - %Y %H : %M : %S %b %d %Y %H : %M : %S %b %d %Y %H - %M - %S %b %d %H : %M : %S %Y %b %d %H - %M - %S %Y %b %d %H : %M : %S %b %d %H - %M - %S %Y %H : %M : %S %Y %H - %M - %S %m - %d - %Y %H : %M : %S %H - %M - %S %Y entspricht einem vierstelligen Jahr. %m entspricht der Nummer des Monats (1 – 12). %d entspricht dem Datum (1 – 31). %H entspricht den Stunden (1 – 24). %M entspricht den Minuten (0 – 60). %S entspricht den Sekunden (0 – 60). %b entspricht der Abkürzung für den Monat (Jan, Feb).

Dies ist ein Beispiel für eine Regel, bei der ein Kennwort aus einer OpenSSH-Anmeldung identifiziert wird. Außerdem werden die Quell-IP-Adresse, der Quell-Port und der Benutzername abgerufen:

```
alert any any any -> any any (msg:"OpenSSH Accepted Password";content:"Accepted
password for ";pcre:"Accepted\s+password\s+for\s+(\S+)\s+from\s+(\d+\.\d+\.\d+\.\d+)\s
+port\s+(\d+)";setparm:username=1;setparm:src_ip=2;setparm:src_port=3;sid:31;rev:1;)
```

Online finden Sie PCRE-Ressourcen unter http://perldoc.perl.org/perlre.html.

Hinzufügen einer ASP-Datenquelle mit abweichender Codierung

In ESM werden mit UTF-8 codierte Daten gelesen. Wenn Sie eine ASP-Datenquelle haben, von der Daten mit abweichender Codierung generiert werden, müssen Sie dies beim Hinzufügen der Datenquelle angeben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der Systemnavigationsstruktur auf einen Empfänger, und klicken Sie dann auf das Symbol **Datenquelle hinzufügen**  .

2 Wählen Sie im Feld **Datenquellenanbieter** die Option **Generisch** und dann im Feld **Datenquellenmodell** die Option **Erweiterter Syslog-Parser** aus.

3 Geben Sie die erforderlichen Informationen ein, und wählen Sie im Feld **Codierung** die richtige Codierung aus.

Die Daten aus dieser Datenquelle werden so formatiert, dass sie vom Empfänger gelesen werden können, wenn sie dort eingehen.

Security Device Event Exchange (SDEE)

Mit dem SDEE-Format können Ereignisse, die von verschiedenen von Sicherheitsgerätetypen generiert werden, standardmäßig beschrieben werden. Gemäß der SDEE-Spezifikation werden SDEE-Ereignisse über die Protokolle HTTP oder HTTPS transportiert. HTTP-Server, auf denen Ereignisinformationen mithilfe von SDEE an Clients bereitgestellt werden, heißen SDEE-Anbieter. Die Initiatoren der HTTP-Anfragen werden als SDEE-Clients bezeichnet.

Cisco hat Erweiterungen für den SDEE-Standard definiert, den sogenannten CIDEE-Standard. Der Empfänger kann als SDEE-Client fungieren und von Cisco-IPS-Systemen (Intrusion Prevention Systems) generierte CIDEE-Daten anfragen.

Im Gegensatz zu den anderen vom Empfänger unterstützten Datenquellentypen wird bei SDEE ein "Pull"-Modell anstelle eines "Push"-Modells verwendet. Dies bedeutet, dass regelmäßig eine Verbindung zwischen dem Empfänger und dem SDEE-Anbieter hergestellt wird. Dabei werden alle Ereignisse angefragt, die seit dem letzten angefragten Ereignis generiert wurden. Die vom SDEE-Anbieter angefragten Ereignisse werden jeweils in der Ereignisdatenbank des Empfängers verarbeitet und gespeichert und können vom ESM-Gerät abgerufen werden.

Sie können einen SDEE-Anbieter zu einem Empfänger hinzufügen, indem Sie Cisco als Anbieter und IOS IPS (SDEE) als Datenquellenmodell auswählen (siehe *Hinzufügen einer Datenquelle*).

Die folgenden Informationen können vom Empfänger aus einem SDEE/CIDEE-Ereignis extrahiert werden:

- Quell- und Ziel IP-Adressen
- Quell- und Ziel-Ports
- Protokoll
- Ereigniszeitpunkt
- Ereignisanzahl (CIDEE bietet eine Art von Ereignisaggregation, die vom Empfänger unterstützt wird.)
- Signatur-ID und Sub-ID
- Die ESM-Ereignis-ID wird mit der folgenden Formel aus der SDEE-Signatur-ID und der CIDEE-Sub-Signatur-ID berechnet:

  ESMI-ID = (SDEE-ID * 1000) + CIDEE-Sub-ID

  Wenn also die SDEE-Signatur-ID 2000 lautet und die CIDEE-Sub-Signatur-ID 123 entspricht, ergibt sich die ESMI-Ereignis-ID 2000123.

- VLAN
- Schweregrad
- Ereignisbeschreibung
- Paketinhalt (falls verfügbar)

Bei der ersten Verbindung zwischen Empfänger und SDEE-Anbieter werden das aktuelle Datum und die aktuelle Uhrzeit als Ausgangspunkt für die Ereignisanfragen verwendet. Bei zukünftigen Verbindungen werden alle Ereignisse angefragt, die seit dem letzten erfolgreichen Abruf aufgetreten sind.

Konfigurieren von ePolicy Orchestrator 4.0

Von der McAfee Event Receiver-Datenquelle für ePolicy Orchestrator wird jetzt ePolicy Orchestrator 4.0 unterstützt. ePolicy Orchestrator In Version 4.0 werden Ereignisse in einer SQL Server-Datenbank gespeichert. Über JDBC wird eine Verbindung zwischen der ePolicy Orchestrator-Datenquelle und dieser SQL Server-Datenbank hergestellt, um Ereignisinformationen abzurufen. Sie müssen in der ePolicy Orchestrator-Datenbank einen neuen Benutzernamen (ID) und ein neues Kennwort erstellen, die in Verbindung mit der Datenquelle für ePolicy Orchestrator verwendet werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Melden Sie sich beim ePolicy Orchestrator-Datenbank-Server an.
2. Starten Sie **SQL Server Enterprise Manager**, indem Sie Folgendes auswählen: **Starten** | **Alle Programme** | **Microsoft SQL Server** | **Enterprise Log Manager**.
3. Erweitern Sie mehrmals den Knoten Konsolenstamm, um die Elemente unter dem Ordner Sicherheit anzuzeigen.
4. Klicken Sie mit der rechten Maustaste auf das Symbol **Anmeldungen**, und wählen Sie dann im Menü die Option **Neue Anmeldung** aus.
5. Geben Sie auf der Seite **SQL Server – Anmeldungseigenschaften – Neue Anmeldung** auf der Registerkarte **Allgemein** Folgendes ein:
   a. Geben Sie in das Feld **Name** den Benutzernamen ein, den Sie für die Datenquelle für ePolicy Orchestrator verwenden möchten, um die Verbindung mit der ePolicy Orchestrator-Datenbank herzustellen (beispielsweise nfepo).
   b. Wählen Sie in **Authentifizierung** die Option **Kennwort für SQL Server-Authentifizierung** aus, und geben Sie dann das Kennwort ein.
   c. Wählen Sie in **Standardwerte** die ePolicy Orchestrator-Datenbank (ePO4_<Hostname>) aus der Dropdown-Liste **Datenbank** aus.

   Wenn Sie den Standardwert **Datenbank** als Master beibehalten, werden von der Datenquelle für ePolicy Orchestrator keine Ereignisse abgerufen.
6. Wählen Sie auf der Registerkarte **Datenbankzugriff** die Option **Zulassen** aus, die der ePolicy Orchestrator-Datenbank zugeordnet ist.
7. Wählen Sie für **Zulassen in Datenbankrolle** die Option **db_datareader** aus, und klicken Sie dann auf **OK**.
8. Bestätigen Sie das neue Kennwort, und klicken Sie dann auf **OK**.

Hinzufügen einer ArcSight-Datenquelle

Fügen Sie Datenquellen für ein ArcSight-Gerät hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur den Knoten des Empfängers aus.
2. Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Datenquelle hinzufügen**  .
3. Wählen Sie im Feld **Datenquellenanbieter** die Option **ArcSight** und dann im Feld **Datenquellenmodell** die Option **Einheitliches Ereignisformat** aus.
4. Geben Sie einen Namen für die Datenquelle und dann die ArcSight-IP-Adresse ein.
5. Füllen Sie die verbleibenden Felder aus (siehe *Hinzufügen einer Datenquelle*).
6. Klicken Sie auf **OK**.
7. Richten Sie für jede Quelle, von der Daten an das ArcSight-Gerät weitergeleitet werden, eine Datenquelle ein.

Die von ArcSight empfangenen Daten werden analysiert, damit sie in der ESM-Konsole angezeigt werden können.

Einheitliches Ereignisformat (CEF)

Zurzeit werden von ArcSight Ereignisse aus 270 Datenquellen mithilfe von intelligenten Konnektoren in das einheitliche Ereignisformat (Common Event Format, CEF) konvertiert. CEF ist ein Interoperabilitätsstandard für Geräte, auf denen Ereignisse oder Protokolle generiert werden. Dieser Standard enthält die relevantesten Geräteinformationen und erleichtert die Analyse und Verwendung von Ereignissen.

Die Ereignisnachricht muss nicht ausdrücklich vom Ereigniserzeuger generiert werden. Die Nachricht wird mit einem allgemeinen Präfix formatiert, das aus durch Pipe-Zeichen (|) getrennten Feldern besteht. Das Präfix ist obligatorisch, und alle angegebenen Felder müssen vorhanden sein. Zusätzliche Felder werden in der Erweiterung angegeben. Das Format lautet:

```
CEF:Version|Geräteanbieter|Geräteprodukt|Geräteversion|Geräte-Ereignisklassen-ID|Name|
Schweregrad|Erweiterung
```

Der Erweiterungsteil der Nachricht ist ein Platzhalter für zusätzliche Felder. Die Präfixfelder werden wie folgt definiert:

- **Version** ist eine Ganzzahl und gibt die Version des CEF-Formats an. Ereignisverbraucher ermitteln anhand dieser Informationen, was die Felder darstellen. Zurzeit wird nur Version 0 (null) im oben genannten Format angegeben. Möglicherweise werden Sie die Erfahrung machen, dass Sie weitere Felder zum "Präfix" hinzufügen müssen und daher die Versionsnummer ändern müssen. Neue Formate werden von dem für den Standard zuständigen Gremium hinzugefügt.
- Mit den Zeichenfolgen **Geräteanbieter**, **Geräteprodukt** und **Geräteversion** wird der Typ des sendenden Geräts eindeutig identifiziert. Das Paar aus Device Vendor und Device Product darf nur jeweils von einem Produkt verwendet werden. Es gibt keine zentrale Stelle für die Verwaltung dieser Paare. Es muss sichergestellt sein, dass von Ereigniserzeugern eindeutige Namenspaare zugewiesen werden.
- **Geräte-Ereignisklassen-ID** ist eine eindeutige ID für den Ereignis-Typ. Dabei kann es sich um eine Zeichenfolge oder eine Ganzzahl handeln. Mit DeviceEventClassId wird der Typ des gemeldeten Ereignisses identifiziert. Bei IDS-Systemen (Intrusion Detection System, System zur Erkennung von Eindringungsversuchen) wird jeder Signatur oder Regel, mit der bestimmte Aktivitäten entdeckt werden, eine eindeutige deviceEventClassId zugewiesen. Diese Anforderung gilt auch für andere Gerätetypen und erleichtert die Behandlung der Ereignisse durch die Korrelationsmodule.

- **Name** ist eine Zeichenfolge, die eine für Menschen lesbare und verständliche Beschreibung des Ereignisses darstellt. Der Ereignisname sollte keine Informationen enthalten, die ausdrücklich in anderen Feldern vorkommen. Beispiel: "Port scan from 10.0.0.1 targeting 20.1.1.1" ist kein guter Name für ein Ereignis. Richtig wäre: "Port scan". Die anderen Informationen sind redundant und können aus den anderen Feldern übernommen werden.
- **Schweregrad** ist eine Ganzzahl, die die Wichtigkeit des Ereignisses angibt. Zulässig sind nur Zahlen von 0 bis 10. Dabei steht 10 für das wichtigste Ereignis.
- **Erweiterung** ist eine Sammlung von Schlüssel-Wert-Paaren. Die Schlüssel sind Bestandteil eines vordefinierten Satzes. Gemäß dem Standard können wie weiter unten beschrieben zusätzliche Schlüssel einbezogen werden. Ein Ereignis kann beliebig viele durch Leerzeichen getrennte Paare aus Schlüssel und Wert in beliebiger Reihenfolge enthalten. Wenn ein Feld ein Leerzeichen enthält, beispielsweise in einem Dateinamen, ist dies zulässig und kann genau so protokolliert werden. Beispiel:

```
fileName=c:\Program Files\ArcSight ist ein gültiges Token.
```

Hier ist eine Beispielnachricht, um die Darstellung zu veranschaulichen:

```
Sep 19 08:26:10 zurich CEF:0|security|threatmanager|1.0|100|worm successfully stopped|
10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

Wenn Sie NetWitness verwenden, muss das Gerät richtig konfiguriert sein, damit die CEF-Nachricht an den Empfänger gesendet wird. Standardmäßig sieht das CEF-Format bei Verwendung von NetWitness so aus:

```
CEF:0|Netwitness|Informer|1.6|{name}|{name}|Medium | externalId={#sessionid}
proto={#ip.proto} categorySignificance=/Normal categoryBehavior=/Authentication/Verify
categoryDeviceGroup=/OS categoryOutcome=/Attempt categoryObject=/Host/Application/
Service act={#action} deviceDirection=0 shost={#ip.host} src={#ip.src}
spt={#tcp.srcport} dhost={#ip.host} dst={#ip.dst} dport={#tcp.dstport}
duser={#username} dproc=27444 fileType=security cs1={#did} cs2={#password} cs3=4 cs4=5
cn1={#rid} cn2=0 cn3=0
```

Für das richtige Format müssen Sie oben "dport" in "dpt" ändern.

Adiscon-Setup

Syslog WMI wird durch Adiscon unterstützt.

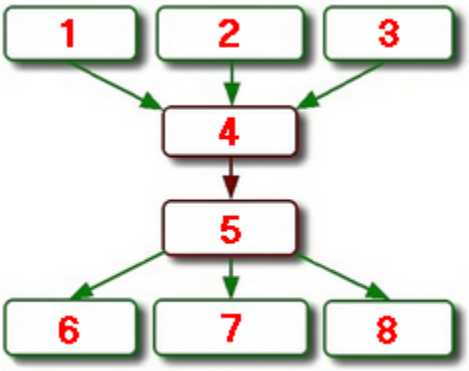
Sie müssen in Event Reporter die folgende Formatzeichenfolge verwenden, damit die Adiscon-Datenquelle für Microsoft Windows-Ereignisse richtig funktioniert:

```
%sourceproc%,%id%,%timereported:::uxTimeStamp%,%user%,%category%,%Param0%;%Param1%;
%Param2%;%Param3%;%Param4%;%Param5%;%Param6%;%Param7%;%Param8%;%Param9%;%Param10%;
%Param11%;%Param12%;%Param13%;%Param14%;%Param15%
```

Unterstützung für Syslog-Relay

Für die Weiterleitung von Ereignissen von verschiedenen Geräten durch einen Syslog-RelayServer an den Empfänger sind zusätzliche Schritte erforderlich.

Sie müssen eine einzige Syslog-Relay-Datenquelle hinzufügen, um den Datenstrom und die zusätzlichen Datenquellen zu akzeptieren. Dann kann der Datenstrom vom Empfänger in die ursprünglichen Datenquellen aufgeteilt werden. Sylog-ng und Splunk werden unterstützt. Im folgenden Diagramm wird das Szenario beschrieben:



1 Cisco ASA-Gerät

2 SourceFire Snort-Gerät

3 TippingPoint-Gerät

4 Syslog-Relay

5 Datenquelle 1: Syslog-Relay

6 Datenquelle 2: Cisco ASA

7 Datenquelle 3: SourceFire Snort

8 Datenquelle 4: TippingPoint

In diesem Beispielszenario müssen Sie die Syslog-Relay-Datenquelle (5) für den Empfang des Datenstroms vom Syslog-Relay (4) einrichten. Dazu wählen Sie im Feld **Syslog-Relay** die Option **Syslog** aus. Wenn die Syslog-Relay-Datenquelle eingerichtet ist, fügen Sie die Datenquellen für die einzelnen Geräte (6, 7 und 8) hinzu. Dazu wählen Sie im Feld **Syslog-Relay** die Option **Keine** aus, da es sich bei diesem Gerät nicht um einen Syslog-RelayServer handelt.

Die Funktion **Syslog-Nachrichten hochladen** kann in einer Syslog-Relay-Konfiguration nicht verwendet werden.

Der Syslog-Header muss so konfiguriert sein, dass er wie im folgenden Beispiel aussieht: `1 <123> 345 Oct 7 12:12:12 2012 mcafee.com httpd[123]`

Dabei gilt Folgendes:

`1` =	Syslog-Version (optional)
`345` =	Syslog-Länge (optional)
`<123>` =	Einrichtung (optional)
`Oct 7 12:12:12 2012` =	Datum. Hier werden Hunderte von Formaten unterstützt (erforderlich).
`mcafee.com`	Hostname oder IP-Adresse (IPv4 oder IPv6, erforderlich)
`httpd` =	Anwendungsname (optional)

[123]	Anwendungs-PID (optional)
: =	Doppelpunkt (optional)

Die Felder für den Hostnamen und die Daten können in beliebiger Reihenfolge angezeigt werden. Eine IPv6-Adresse kann in eckige Klammern [ ] eingeschlossen werden.

Ausführen des NSM-SIEM-Konfigurations-Tools

Vor dem Einrichten einer NSM-Datenquelle müssen Sie das NSM-SIEM-Konfigurations-Tool ausführen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Laden Sie das Konfigurations-Tool herunter.
   a. Navigieren Sie zur McAfee-Website für Produkt-Downloads.
   b. Geben Sie in das Suchfeld **Meine Produkte herunterladen** die Kunden-Grant-Nummer ein, die Sie erhalten haben.
   c. Klicken Sie auf **Suchen**. Die Produktaktualisierungsdateien befinden sich unter dem Download-Link MFE **<Produktname> <Version>**.
   d. Lesen Sie den McAfee-Endbenutzer-Lizenzvertrag, und klicken Sie auf **Ich stimme zu**.
   e. Laden Sie die Dateien für das **NSM-SIEM-Konfigurations-Tool** herunter.
2. Führen Sie das Konfigurations-Tool auf dem NSM-Server aus.

   Der Standardpfad zu NSM muss für das Tool auffindbar sein. Wenn der Pfad nicht gefunden wird, navigieren Sie zu NSM.
3. Geben Sie den NSM SQL-Benutzernamen und das entsprechende Kennwort sowie den bei der Installation von NSM eingegebenen Datenbanknamen ein.
4. Geben Sie den SIEM-Benutzernamen und das zugehörige Kennwort für die Datenquelle sowie die IP-Adresse des Empfängers, auf dem die Datenquelle hinzugefügt wird, ein.

Diese Informationen geben Sie auf dem Bildschirm der Datenquelle ein.

Einrichten von ePolicy Orchestrator

Sie können mehrere ePolicy Orchestrator-Datenquellen einrichten, die alle auf die gleiche IP-Adresse verweisen und für die im Feld für den Datenbanknamen unterschiedliche Namen angegeben sind.

Auf diese Weise können Sie beliebig viele ePolicy Orchestrator-Datenquellen einrichten und alle auf verschiedene Datenbanken auf dem zentralen Server zeigen lassen. Geben Sie in die Felder **Benutzer-ID** und **Kennwort** die Informationen für den Zugriff auf die ePolicy Orchestrator-Datenbank und in das Feld **Version** die Version des ePolicy Orchestrator-Geräts ein. Der Standard-Port lautet 1433.

Das Feld **Datenbankname** ist erforderlich. Wenn der Datenbankname einen Bindestrich enthält, müssen Sie den Namen in eckige Klammern einschließen (beispielsweise [ePO4_WIN-123456]).

Mit der Option **ePO-Abfrage** können Sie eine Abfrage an das ePolicy Orchestrator-Gerät senden und Client-Datenquellen erstellen. Wenn im Feld **Client-Datenquellen verwenden** die Standardeinstellung **Vergleich nach Typ** ausgewählt ist und Sie auf **ePO-Abfrage** klicken, wird eine Abfrage an das ePolicy Orchestrator-Gerät gesendet, und alle unterstützten ePolicy Orchestrator-Produkte werden als Client-Datenquellen hinzugefügt.

Die folgenden Produkte werden unterstützt, wenn sie vollständig in ePolicy Orchestrator integriert sind:

- ANTISPYWARE
- DLP
- EPOAGENT
- GSD
- GSE
- HOSTIPS
- MNAC
- POLICYAUDITOR
- SITEADVISOR
- VIRUSCAN
- SOLIDCORE

Wenn **IP vergleichen** ausgewählt ist, wird eine Abfrage an das ePolicy Orchestrator-Gerät gesendet, und für alle Endpunkte in der ePolicy Orchestrator-Datenbank werden Client-Datenquellen erstellt. Wenn in der ePolicy Orchestrator-Datenbank mehr als 256 Endpunkte vorhanden sind, werden mehrere Datenquellen mit Clients erstellt.

McAfee Risk Assessment-Daten wird von ePolicy Orchestrator-Servern erfasst. Sie können mehrere ePolicy Orchestrator-Server festlegen, von denen die McAfee Risk Advisor- Daten erfasst werden sollen. Die McAfee Risk Advisor-Daten werden über eine Datenbankabfrage aus der SQL Server-Datenbank von ePolicy Orchestrator erfasst. Aus der Datenbankabfrage ergibt sich eine Liste mit einer Gegenüberstellung von IP und Reputationsfaktor. Außerdem werden Konstantenwerte für die hohen und niedrigen Reputationswerte bereitgestellt. Alle Listen aus ePolicy Orchestrator und McAfee Risk Advisor werden zusammengeführt. Dabei erhalten doppelte IPs den höchsten Faktor. Die zusammengeführte Liste wird mit den niedrigen und hohen Werten an alle ACE-Geräte gesendet, die für die Bewertung von SrcIP- und DstIP-Feldern verwendet werden.

Wenn Sie eine ePolicy Orchestrator-Datenquelle hinzufügen und auf **OK** klicken, um sie zu speichern, werden Sie gefragt, ob Sie die Datenquelle zum Konfigurieren von McAfee Risk Advisor-Daten verwenden möchten. Wenn Sie auf **Ja** klicken, werden eine Datenanreicherungsquelle und (gegebenenfalls) zwei ACE-Bewertungsregeln erstellt und ein entsprechender Rollout ausgeführt. Zum Anzeigen dieser Elemente wechseln Sie zu den Seiten **Datenanreicherung aktivieren** und **Risikokorrelations-Bewertung**. Zum Verwenden der Bewertungsregeln müssen Sie einen Risikokorrelations-Manager erstellen (siehe *Hinzufügen eines Risikokorrelations-Managers*).

IBM Internet Security System SiteProtector

Mit dem Empfänger können Ereignisse von einem Internet Security Systems (ISS) SiteProtector-Server abgerufen werden. Dabei werden Abrufe an die zum Speichern der SiteProtector-Ereignisse verwendete Microsoft SQL Server-Datenbank gesendet.

Im Gegensatz zu anderen vom Empfänger unterstützten Datenquellentypen wird beim Abrufen von Ereignissen von einem SiteProtector-Server ein "Pull"-Modell anstelle eines "Push"-Modells verwendet. Dies bedeutet, dass regelmäßig eine Verbindung zwischen dem Empfänger und der SiteProtector-Datenbank hergestellt wird. Dabei werden alle neuen Ereignisse seit dem letzten abgerufenen Ereignis angefragt. Die vom SiteProtector-Server abgerufenen Ereignisse werden jeweils in der Ereignisdatenbank des Empfängers verarbeitet und gespeichert und können vom ESM-Gerät abgerufen werden.

Für den Gerätetyp stehen zwei Optionen zur Verfügung: **Server** und **Verwaltetes Gerät**. Um Ereignisse von einem SiteProtector-Server zu sammeln, müssen Sie mindestens eine Datenquelle mit dem Gerätetyp Server einrichten.

Wenn eine SiteProtector-Server-Datenquelle konfiguriert ist, werden alle aus SiteProtector gesammelten Daten als zu dieser Datenquelle gehörend angezeigt. Dabei spielt es keine Rolle, von welcher Ressource das Ereignis tatsächlich an den SiteProtector-Server gemeldet wurde. Um

Ereignisse weiter nach der verwalteten Ressource zu kategorisieren, von der das Ereignis an SiteProtector gemeldet wurde, können Sie zusätzliche SiteProtector-Datenquellen auswählen und für diese den Gerätetyp **Verwaltetes Gerät** auswählen.

Mit der unten auf der Seite angezeigten Option **Erweitert** können Sie eine URL definieren, die zum Starten bestimmter URLs beim Anzeigen von Ereignisdaten verwendet werden kann. Außerdem können Sie einen Anbieter, ein Produkt und eine Version definieren, die für die CEF-Weiterleitung (Common Event Format, Einheitliches Ereignisformat) verwendet werden sollen. Diese Einstellungen sind optional.

Damit Ereignisse aus der SiteProtector-Datenbank vom Empfänger abgefragt werden können, müssen von der Microsoft SQL Server-Installation, in der die von SiteProtector verwendete Datenbank gehostet wird, Verbindungen über das TCP/IP-Protokoll zulässig sein.



Die Schritte zum Aktivieren des Protokolls und zum Definieren des für diese Verbindung verwendeten Ports finden Sie in der Dokumentation für Microsoft SQL Server (der Standardwert lautet Port 1433).

Bei der ersten Verbindung zwischen dem Empfänger und der SiteProtector-Datenbank werden nach dem aktuellen Zeitpunkt generierte neue Ereignisse abgerufen. Bei zukünftigen Verbindungen werden alle Ereignisse angefragt, die seit dem letzten erfolgreich abgerufenen Ereignis aufgetreten sind.

Die folgenden Informationen werden vom Empfänger aus einem SiteProtector-Ereignis extrahiert:

- Quell- und Ziel IP-Adressen (IPv4)
- Quell- und Ziel-Ports
- Protokoll
- Ereigniszeitpunkt
- Ereignisanzahl
- VLAN
- Schweregrad
- Ereignisbeschreibung

Einrichten von Check Point

Richten Sie Datenquellen ein, die Anbieter 1, Check Point-Hochverfügbarkeit und die meisten Check Point-Standardumgebungen abdecken.

Im ersten Schritt fügen Sie die übergeordnete Check Point-Datenquelle hinzu (siehe *Hinzufügen einer Datenquelle*). Wenn die übergeordnete Datenquelle nicht als Protokoll-Server fungiert und Sie einen dedizierten Protokoll-Server verwenden, müssen Sie eine Datenquelle für den Protokoll-Server hinzufügen. Fügen Sie außerdem nach Bedarf untergeordnete Datenquellen hinzu. In einer Hochverfügbarkeitsumgebung müssen Sie für jedes sekundäre SMS/CMA-Gerät eine untergeordnete Datenquelle hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Fügen Sie eine übergeordnete Datenquelle für das SMS/CMA-Gerät, auf dem die OPSEC-Anwendung bzw. das OPSEC-Zertifikat gespeichert ist. Wenn Sie Empfänger-HA verwenden, fügen Sie eine übergeordnete Datenquelle für das primäre SMS/CMA-Gerät hinzu.

   OPSEC ist nicht FIPS-konform. Verwenden Sie diese Funktion nicht, wenn Sie FIPS-Vorschriften einhalten müssen (siehe *Anhang A*).

2. Klicken Sie auf **Optionen**.
3. Wählen Sie auf der Seite **Erweiterte Einstellungen** die Kommunikationsmethode aus, und geben Sie dann in **Eindeutiger Name der Server-Entität** den entsprechenden Namen der Datenquelle ein.
4. Klicken Sie zweimal auf **OK**.

5 Führen Sie gegebenenfalls die folgenden Schritte aus:

Fehlermeldung	Abhilfemaßnahme
SIC-Fehler für LEA: Client could not choose an authentication method for service lea (Vom Client konnte keine Authentifizierungsmethode für den Dienst LEA ausgewählt werden).	1 Vergewissern Sie sich, dass Sie beim Hinzufügen der Check Point-Datenquelle die richtigen Einstellungen für **Authentifizierung verwenden** und **Verschlüsselung verwenden** ausgewählt haben. Wenn Sie nur **Authentifizierung verwenden** ausgewählt haben, wird vom OPSEC-Client "sslca_clear" für die Kommunikation mit dem Protokoll-Server verwendet. Wenn Sie **Authentifizierung verwenden** und **Verschlüsselung verwenden** ausgewählt haben, wird vom OPSEC-Client "sslca" für die Kommunikation mit dem Protokoll-Server verwendet. Wenn Sie keine der beiden Optionen ausgewählt haben, wird die vom OPSEC-Client "keine" für die Kommunikation mit dem Protokoll-Server verwendet. 2 Vergewissern Sie sich, dass in der OPSEC-Anwendung, die Sie für die Kommunikation mit dem Check Point-Protokoll-Server verwenden, im Abschnitt für **Client Entities** (Client-Entitäten) die Option **LEA** ausgewählt ist. 3 Wenn in beiden Schritten die richtigen Optionen ausgewählt sind, suchen Sie in der Installation des Check Point-Protokoll-Servers die Datei sic_policy.conf. Auf einem Linux-basierten R65-System beispielsweise befindet sich die Datei in /var/opt/CPshrd-R65/conf. 4 Wenn Sie ermittelt haben, mit welcher Kommunikationsmethode (Authentifizierungsmethode in der Datei) die LEA-Kommunikation mit dem Protokoll-Server möglich ist, wählen Sie diese Kommunikationsmethode auf der Seite **Erweiterte Einstellungen** als **Kommunikationsmethode** aus.
SIC-Fehler für LEA: Vom Peer wurde ein falscher eindeutiger Name (DN) gesendet: <erwarteter eindeutiger Name>	• Geben Sie in das Textfeld **Eindeutiger Name der Server-Entität** die Zeichenfolge ein, die "<erwarteter eindeutiger Name>" in der Fehlermeldung entspricht. Alternativ können Sie den eindeutigen Namen für den Check Point-Protokoll-Server ermitteln, indem Sie das Netzwerkobjekt des Check Point-Protokoll-Servers auf der Benutzeroberfläche von Smart Dashboard überprüfen. Der eindeutige Name des SMS/CMA-Geräts sieht ähnlich aus wie der für die OPSEC-Anwendung. Lediglich der erste Eintrag wird durch CN=cp_mgmt ersetzt. Angenommen, die OPSEC-Anwendung hat den eindeutigen Namen CN=mcafee_OPSEC,O=r75..n55nc3. Der eindeutige Name des SMS/CMA-Geräts lautet dann CN=cp_mgmt,O=r75..n55nc3. Der eindeutige Name des Protokoll-Servers lautet CN=CPlogserver,O=r75..n55nc3.

6 Fügen Sie für alle Firewalls, Protokoll-Server oder sekundären SMS/CMA-Geräte, die von der eingerichteten übergeordneten Datenquelle verwaltet werden, eine untergeordnete Datenquelle hinzu (siehe *Hinzufügen einer untergeordneten Datenquelle*).

Der Gerätetyp für alle Firewall/-Gateway-Datenquellen lautet **Sicherheitsgerät**. Als Standardeinstellung für **Übergeordnete Berichtskonsole** wird die übergeordnete Datenquelle festgelegt.

McAfee-Regelsätze

In dieser Tabelle finden Sie die McAfee-Regelsätze sowie die externen Datenquellen-IDs.

Datenquellen-ID	Anzeigename	Entsprechende RSID	Regelbereich
50201	Firewall	0	2,000,000–2,099,999
50202	Benutzerdefinierte Firewall	0	2,200,000–2,299,999
50203	Benutzerdefinierte Signaturen	0	5,000,000–5,999,999
50204	Intern	0	3,000,000–3,999,999
50205	Schwachstelle und Exploit	2	Nicht zutreffend
50206	Nicht jugendfreie Inhalte	5	Nicht zutreffend
50207	Chat	8	Nicht zutreffend
50208	Richtlinie	11	Nicht zutreffend
50209	Peer-to-Peer	14	Nicht zutreffend
50210	Multimedia	17	Nicht zutreffend
50211	Alpha	25	Nicht zutreffend
50212	Virus	28	Nicht zutreffend
50213	Perimeter Secure Application	31	Nicht zutreffend
50214	Gateway	33	Nicht zutreffend
50215	Malware	35	Nicht zutreffend
50216	SCADA	40	Nicht zutreffend
50217	MCAFEESYSLOG	41	Nicht zutreffend

Empfängerressourcenquellen

Eine Ressource ist ein beliebiges Gerät im Netzwerk, das über eine IP-Adresse verfügt. Auf der Registerkarte **Ressource** in **Asset Manager** können Sie Ressourcen erstellen, ihre Tags ändern, Ressourcengruppen erstellen, Ressourcenquellen hinzufügen und eine Ressource zu einer Ressourcengruppe hinzufügen. Außerdem können Sie die Ressourcen ändern, die von einem der VA-Anbieter erlernt wurden.

Mit der Funktion **Ressourcenquellen** unter **Empfängereigenschaften** können Sie gegebenenfalls Daten aus **Active Directory** abrufen. Nach Abschluss des Prozesses können Sie Ereignisdaten filtern, indem Sie die abgerufenen Benutzer oder Gruppen in den Abfragefilterfeldern **Quellbenutzer** und **Zielbenutzer für Ansichten** auswählen. Auf diese Weise können Sie leichter Compliance-Daten für Anforderungen wie beispielsweise PCI bereitstellen. Für ein ESM-Gerät kann nur eine Ressourcenquelle festgelegt sein. Für Empfänger können mehrere Ressourcenquellen verwendet werden.

Wenn von zwei Ressourcenerkennungsquellen (beispielsweise Vulnerability Assessment und Netzwerkerkennung) die gleiche Ressource gefunden wird, wird die entdeckte Ressource von der Erkennungsmethode mit der höchsten Priorität zur Tabelle hinzugefügt. Wenn zwei Erkennungsquellen die gleiche Priorität haben, hat diejenige Vorrang, von der die Ressource zuletzt gefunden wurde.

Hinzufügen einer Ressourcenquelle

Zum Abrufen von Daten aus **Active Directory** müssen Sie einen Empfänger konfigurieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Empfängereigenschaften** aus, und klicken Sie dann auf **Ressourcenquellen**.

2 Klicken Sie auf **Hinzufügen**, und geben Sie dann die erforderlichen Informationen ein.

3 Klicken Sie auf **OK** und dann auf der Seite **Ressourcenquellen** auf **Schreiben**.

Einstellungen für Enterprise Log Manager (ELM)

In ELM wird das Speichern und Verwalten von Protokolldaten, der Zugriff auf Protokolldaten und die Berichterstellung für Protokolldaten unterstützt.

Die von ELM empfangenen Daten werden in Speicherpools organisiert, die jeweils aus Speichergeräten bestehen. Jedem Speicherpool wird eine Aufbewahrungsdauer zugeordnet, und die Daten werden während dieses Zeitraums im Pool beibehalten. Protokolle müssen aufgrund von Vorschriften von Behörden, Branchen und Unternehmen unterschiedlich lange gespeichert werden.

Sie können für das ELM-Gerät Suchaufträge und Integritätsprüfungsaufträge einrichten. Bei jedem dieser Aufträge wird auf die gespeicherten Protokolle zugegriffen, und die im Auftrag definierten Daten werden abgerufen oder überprüft. Anschließend können Sie die Ergebnisse anzeigen und wahlweise die Informationen exportieren.

Die bereitgestellten Informationen gelten für alle folgenden ELM-Gerätemodelle:

- ENMELM-5205 (Kombination aus ESM und Log Manager)
- ENMELM-5510 (Kombination aus ESM und Log Manager)
- ENMELM-4245 (Kombination aus ESM und Log Manager)
- ELM-5205
- ELM-5510
- ELM-5750
- ELMERC-4245 (Kombination aus Empfänger und Log Manager)
- ELMERC-2250 (Kombination aus Empfänger und Log Manager)
- ELMERC-2230 (Kombination aus Empfänger und Log Manager)

Zum Konfigurieren eines ELM-Geräts benötigen Sie die folgenden Informationen:

- Die Quellen, deren Protokolle auf dem ELM-Gerät gespeichert werden.
- Die erforderlichen Speicherpools und die jeweilige Datenbeibehaltungsdauer
- Die zum Speichern der Daten erforderlichen Speichergeräte

Im Allgemeinen kennen Sie die Quellen, deren Protokolle auf dem ELM-Gerät gespeichert werden, und die erforderlichen Speicherpools. Sie wissen jedoch nicht, welche Speichergeräte zum Speichern der Daten benötigt werden. Diese Ungewissheit räumen Sie am besten wie folgt aus:

1 Erstellen Sie eine vorsichtige Schätzung des Speicherbedarfs.



Ab Version 9.0.0 sind in ELM-Speicherpools 10 % des zugeordneten Speicherplatzes als Overhead für die Spiegelung erforderlich. Achten Sie darauf, diese 10 % bei der Berechnung des erforderlichen Speicherplatzes zu berücksichtigen.

2 Konfigurieren Sie ELM-Speichergeräte gemäß den geschätzten Anforderungen.

3 Erfassen Sie über einen kurzen Zeitraum Protokolle auf dem ELM-Gerät.

4 Ändern Sie die Konfigurationen der Speichergeräte anhand der ELM-Speicherplatzstatistik so, dass sie im Einklang mit den tatsächlichen Anforderungen an den Datenspeicher stehen.

Vorbereiten der Speicherung von Daten auf dem ELM-Gerät

Sie müssen verschiedene Schritte ausführen, um ein ELM-Gerät für die Speicherung von Daten zu konfigurieren.

Schritt	Aktion	Beschreibung
1	Definieren der Datenbeibehaltungsdauer	Definieren Sie abhängig von den ELM-Installationsanforderungen die Anzahl der verschiedenen benötigten Angaben für die Datenbeibehaltungsdauer. Gängige Angaben für die Datenbeibehaltungsdauer: • SOX: 7 Jahre • PCI: 1 Jahr • GLBA: 6 Jahre • EU-Direktive für die Datenbeibehaltung: 2 Jahre • Basel II: 7 Jahre • HIPAA: 6 oder 7 Jahre • NERC: 3 Jahre • FISMA: 3 Jahre
2	Definieren von Quellen für Protokolldaten	Das Ziel besteht hier darin, alle Quellen für auf dem ELM-Gerät gespeicherte Protokolle zu definieren und für jede Quelle die durchschnittliche Größe der Protokolle in Byte sowie die durchschnittliche Anzahl der pro Tag generierten Protokolle zu schätzen. Hier ist nur eine Schätzung notwendig. Möglicherweise fällt es Ihnen leichter, die durchschnittliche Größe der Protokolle in Byte und die durchschnittliche Anzahl der pro Tag generierten Protokolle für Quellentypen (beispielsweise Firewall, Router, Nitro IPS, ADM, DEM, ELM) und dann die Anzahl der Quellen pro Typ zu schätzen. Im nächsten Schritt müssen Sie die einzelnen Quellen einer in Schritt 1 definierten Beibehaltungsdauer zuordnen. Achten Sie daher darauf, dies beim Schätzen der Quellentypen zu berücksichtigen (beispielsweise SOX-Firewall, PCI-DEM).
3	Definieren von Speicherpools	Ordnen Sie basierend auf den ELM-Installationsanforderungen die einzelnen Protokollquellen oder Quellen einer Datenbeibehaltungsdauer zu. Definieren Sie dabei die Gruppe der für die ELM-Installation erforderlichen Speicherpools.

Schritt	Aktion	Beschreibung
4	Schätzen der Anforderungen für die Speicherpoolgröße	Schätzen Sie mithilfe einer der folgenden Gleichungen den Speicherbedarf für die einzelnen Speicherpools: • Verwendung einzelner Quellen: IRSGB = 0,1*(DRTD*SUM(DSAB*DSALPD))/ (1024*1024*1024) Dabei gilt Folgendes: IRSGB = Anfänglich erforderlicher Speicherplatz in GB DRTD = Dauer der Datenbeibehaltung in Tagen SUMME() = Summe für alle Datenquellen DSAB = Durchschnittliche Anzahl der Bytes in Datenquellen pro Protokoll DSALPD = Durchschnittliche Anzahl der Protokolle von Datenquellen pro Tag • Verwendung von Quellentypen: IRSGB = 0,1*(DRTD*SUM(NDS*DSTAB*DSTALPD))/ (1024*1024*1024) Dabei gilt Folgendes: IRSGB = Anfänglich erforderlicher Speicherplatz in GB DRTD = Dauer der Datenbeibehaltung in Tagen NDS = Anzahl der Datenquellen eines Datenquellentyps SUMME() = Summe für alle Datenquellentypen DSTAB = Durchschnittliche Anzahl der Bytes in Datenquellentypen pro Protokoll DSTALPD = Durchschnittliche Anzahl der Protokolle von Datenquellentypen pro Tag
5	Erstellen der anfänglichen Speichergeräte	Erstellen Sie mindestens ein ELM-Speichergerät, damit genug Speicherplatz für die einzelnen Datenmengen (IRSGB) verfügbar ist (siehe *Hinzufügen eines Speichergeräts*).
6	Erstellen von Speicherpools	Erstellen Sie für jeden in Schritt 3 definierten Speicherpool einen ELM-Speicherpool. Verwenden Sie dabei die zugeordnete Beibehaltungsdauer aus Schritt 1, die zugeordneten IRSGB-Werte aus Schritt 4 und die zugeordneten Speichergeräte aus Schritt 5 (siehe *Hinzufügen eines Speicherpools*).
7	Starten der Protokollierung von Daten	Konfigurieren Sie Quellen so, dass ihre Protokolle an das ELM-Gerät gesendet werden. Warten Sie ein oder zwei Tage ab.
8	Optimieren der geschätzten Anforderungen für die Speicherpoolgröße	Optimieren Sie für jeden in Schritt 6 definierten Speicherpool mithilfe der folgenden Gleichung den zugehörigen geschätzten Speicherbedarf: RSGB = 1,1*DRTD*SPABRPD/(1024*1024*1024) Dabei gilt Folgendes: RSGB = Erforderlicher Speicherplatz in GB DRTD = Dauer der Datenbeibehaltung in Tagen SPABRPD = Wert der täglichen durchschnittlichen Byte-Rate des Speicherpools aus dem Statistikbericht

Schritt	Aktion	Beschreibung
9	Ändern oder Erstellen von Speichergeräten	Ändern oder erstellen Sie für jeden RSGB-Wert aus Schritt 8 ELM-Speichergeräte so, dass diese groß genug sind, um die mit RSGB angegebene Datenmenge zu speichern.
10	Ändern von Speicherpools	Ändern Sie bei Bedarf die einzelnen in Schritt 6 erstellten Speicherpools, indem Sie in Schritt 9 erstellte Speichergeräte hinzufügen oder die vorhandene Zuordnung von Speichergeräten erhöhen.

Einrichten von ELM-Speicher

Zum Speichern von Protokollen benötigt das ELM-Gerät Zugriff auf mindestens ein Speichergerät. Der Speicherbedarf für eine ELM-Installation wird anhand der Anzahl der Datenquellen, der entsprechenden Protokollierungsmerkmale und der entsprechenden Anforderungen an die Dauer der Datenbeibehaltung berechnet. Der Speicherbedarf variiert im Lauf der Zeit, da sich vermutlich alle diese Aspekte während der Lebensdauer einer ELM-Installation ändern.

Details zum Schätzen und Anpassen des Speicherbedarfs für ein System finden Sie unter *ELM-Einstellungen*.

Terminologie im Zusammenhang mit dem ELM-Speicher

Die folgenden Begriffe sollten Sie beim Arbeiten mit ELM-Speicher kennen:

- **Speichergerät**: Ein Datenspeichergerät, auf das von einem ELM-Gerät zugegriffen werden kann. Einige ELM-Modelle verfügen über ein integriertes Speichergerät, andere über die Möglichkeit, einen SAN-Verbindung herzustellen, und manche bieten beides. Alle ELM-Modelle verfügen über die Möglichkeit, eine NAS-Verbindung herzustellen.
- **Speicherzuordnung**: Eine konkrete Datenspeichermenge auf einem bestimmten Speichergerät (beispielsweise 1 TB auf einem NAS-Speichergerät)
- **Dauer der Datenbeibehaltung**: Gibt an, wie lange ein Protokoll gespeichert wird.
- **Speicherpool**: Eine oder mehrere Speicherzuordnungen, die zusammen die gesamte Speichermenge angeben, in Kombination mit einer Datenbeibehaltungsdauer, aus der hervorgeht, wie viele Tage lang ein Protokoll maximal gespeichert werden soll.
- **Protokollquelle**: Eine Quelle für Protokolle, die auf einem ELM-Gerät gespeichert werden.

ELM-Speichergerätetypen

Wenn Sie ein Speichergerät zu einem ELM-Gerät hinzufügen, müssen Sie den Typ des Geräts auswählen. Beim Hinzufügen oder Bearbeiten des Geräts sind einige Punkte zu berücksichtigen.

Gerätetyp	Details
NFS	Wenn Sie den Remote-Bereitstellungspunkt des Speichergeräts mit der ELM-Verwaltungsdatenbank bearbeiten müssen, verschieben Sie die Datenbank mit der Option Datenbank migrieren auf ein anderes Speichergerät (siehe *Migrieren der ELM-Datenbank*). Anschließend können Sie das Feld für den Remote-Bereitstellungspunkt gefahrlos ändern und die Datenbank wieder auf das aktualisierte Speichergerät verschieben.
CIFS	• Wenn Sie den Freigabetyp CIFS mit höheren Samba-Server-Versionen als 3.2 verwenden, kann es zu Datenverlusten kommen. • Verwenden Sie beim Herstellen einer Verbindung mit einer CIFS-Freigabe keine Kommas im Kennwort. • Wenn Sie einen Windows 7-Computer als CIFS-Freigabe verwenden, finden Sie weitere Informationen unter *Deaktivieren der Dateifreigabe für die Heimnetzgruppe*.

Gerätetyp	Details
iSCSI	• Verwenden Sie beim Herstellen einer Verbindung mit einer iSCSI-Freigabe keine Kommas im Kennwort. • Der Versuch, mehrere Geräte mit einem IQN zu verbinden, kann zu Datenverlusten und anderen Konfigurationsproblemen führen.
SAN	Die Option SAN ist nur verfügbar, wenn im ELM-Gerät eine SAN-Karte installiert ist und SAN-Volumes verfügbar sind.

Deaktivieren der Dateifreigabe für die Heimnetzgruppe

In Windows 7 müssen Sie die Dateifreigabe für die Heimnetzgruppe verwenden, die auf anderen Windows 7-Computern, aber nicht mit Samba funktioniert. Um einen Windows 7-Computer als CIFS-Freigabe zu verwenden, müssen Sie die Dateifreigabe für die Heimnetzgruppe deaktivieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Öffnen Sie in Windows 7 die **Systemsteuerung**, und wählen Sie dann **Netzwerk- und Freigabecenter** aus.
2. Klicken Sie auf **Erweiterte Freigabeeinstellungen ändern**.
3. Klicken Sie auf das Profil **Privat oder Arbeitsplatz**, und vergewissern Sie sich, dass es als aktuelles Profil gekennzeichnet ist.
4. Aktivieren Sie die Netzwerkerkennung, die Datei- und Druckerfreigabe und den öffentlichen Ordner.
5. Wechseln Sie zu dem Ordner, den Sie mit CIFS freigeben möchten (versuchen Sie es zuerst mit dem öffentlichen Ordner), und klicken Sie mit der rechten Maustaste auf den Ordner.
6. Wählen Sie **Eigenschaften** aus, und klicken Sie dann auf die Registerkarte **Freigabe**.
7. Klicken Sie auf **Erweiterte Freigabe**, und wählen Sie dann **Diesen Ordner freigeben** aus.
8. (Optional) Ändern Sie den Freigabenamen, und klicken Sie auf **Berechtigungen**.

   Vergewissern Sie sich, dass die Berechtigungen wie gewünscht festgelegt sind (ein Häkchen unter Ändern bedeutet, dass Schreibvorgänge möglich sind). Wenn Sie kennwortgeschützte Freigaben aktiviert haben, müssen Sie die Einstellungen hier anpassen, um sicherzustellen, dass der Ubuntu-Benutzer in den Berechtigungen enthalten ist.

Hinzufügen eines Speichergeräts für die Verknüpfung mit einem Speicherpool

Zum Hinzufügen eines Speichergeräts zur Liste der Speicherorte müssen Sie die Parameter definieren.

Beim Bearbeiten eines Speichergeräts können Sie die Größe erhöhen, aber nicht verringern. Ein Gerät, auf dem Daten gespeichert werden, kann nicht gelöscht werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Speicherpools**.
2. Klicken Sie neben der oberen Tabelle auf **Hinzufügen**.
3. Geben Sie auf der Seite **Speichergerät hinzufügen** die erforderlichen Informationen ein.
4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

   Das Gerät wird zur Liste der verfügbaren ELM-Speichergeräte hinzugefügt.

In der Tabelle auf der Seite **Speicherpools** können Sie Speichergeräte bearbeiten oder löschen.

Hinzufügen oder Bearbeiten eines Speicherpools

Ein Speicherpool enthält mindestens eine Speicherzuordnung und eine Datenbeibehaltungsdauer. Fügen Sie diese zum ELM-Gerät hinzu, um festzulegen, wo ELM-Protokolle gespeichert werden und wie lange sie beibehalten werden müssen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Speicherpool**.
2. Klicken Sie neben der unteren Tabelle auf **Hinzufügen** oder **Bearbeiten**, und geben Sie dann die erforderlichen Informationen ein, oder ändern Sie sie.
3. Klicken Sie auf **OK**.

Sie können die gespeicherten Parameter bearbeiten, und Sie können einen Speicherpool löschen, solange in diesem und auf den zugeordneten Geräten keine Daten gespeichert werden.

Verschieben eines Speicherpools

Sie können einen Speicherpool von einem Gerät auf ein anderes verschieben.

> **Bevor Sie beginnen**
>
> Richten Sie das Speichergerät, auf das Sie den Speicherpool verschieben möchten, als Spiegelung des Geräts ein, auf dem sich der Pool zurzeit befindet (siehe *Hinzufügen eines gespiegelten ELM-Datenspeichers*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das ELM-Gerät aus, auf dem sich der Speicherpool befindet, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Speicherpools**.
3. Klicken Sie in der Tabelle **Speicherpools** auf die gespiegelten Geräte, die unter dem zu verschiebenden Pool aufgeführt sind.
4. Klicken Sie auf **Bearbeiten**, und wählen Sie in der Dropdown-Liste **Datenspeichergeräte** das Gerät aus, auf dem der zu verschiebende Speicherpool gespiegelt wird.

   Dieses Gerät ist nun das Hauptspeichergerät für Daten.
5. Zum Spiegeln des neuen Datenspeichergeräts wählen Sie in der Dropdown-Liste **Gespiegeltes Datenspeichergerät** ein Gerät aus, und klicken Sie dann auf **OK**.

Verringern der Zuordnungsgröße für den Speicher

Wenn ein Speichergerät voll ist, da Speicherplatz für Speicherpools zugeordnet ist, müssen Sie möglicherweise die für die einzelnen Zuordnungen definierte Speicherplatzmenge verringern. Dies

kann notwendig sein, um Speicherplatz auf diesem Gerät für weitere Speicherpools oder für die Volltextindizierung zuzuordnen.

Wenn sich die Verringerung der Zuordnungsgröße auf Daten auswirkt und entsprechender Speicherplatz verfügbar ist, werden die Daten in andere Zuordnungen im Pool verschoben. Wenn der entsprechende Speicherplatz nicht verfügbar ist, werden die ältesten Daten gelöscht.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Speicherpool**.
2. Wählen Sie in der unteren Tabelle den zu verringernden Pool aus, und klicken Sie dann auf **Größe verringern**.
3. Geben Sie ein, um wie viel Sie den Speicher verringern möchten, und klicken Sie dann auf **OK**.

Spiegeln des ELM-Datenspeichers

Sie können ein zweites ELM-Speichergerät einrichten, um die auf dem Hauptgerät erfassten Daten zu spiegeln.

Wenn das Hauptgerät aus irgendeinem Grund ausfällt, werden die eingehenden Daten auf dem Sicherungsgerät weiterhin gespeichert. Wenn das Hauptgerät wieder aktiv ist, wird es automatisch mit der Sicherung synchronisiert. Anschließend wird die Speicherung der eingehenden Daten wieder aufgenommen. Bein einem dauerhaften Ausfall des Hauptgeräts können Sie das Sicherungsgerät auf dem ESM-Gerät als Hauptgerät neu zuweisen und dann für die Spiegelung ein anderes Gerät festlegen.

Wenn eines der Geräte ausfällt, wird in der Systemnavigationsstruktur neben dem ELM-Gerät eine Kennzeichnung für den Integritätsstatus angezeigt.

Möglicherweise wird die Verbindung zwischen einem gespiegelten Speicherpool und dem zugehörigen Speichergerät getrennt. Mögliche Ursachen:

- Der Datei-Server oder das Netzwerk zwischen dem ELM-Gerät und dem Datei-Server ist ausgefallen.
- Der Datei-Server oder das Netzwerk wurde zu Wartungszwecken heruntergefahren.
- Eine Zuordnungsdatei wurde versehentlich gelöscht.

Bei einem Problem mit der Spiegelung wird auf den Speichergeräten ein Warnsymbol in der Tabelle **Speicherpools** angezeigt. Sie können die Spiegelung mit der Funktion **Erneut erstellen** reparieren.

Hinzufügen eines gespiegelten ELM-Datenspeichers

Zum Spiegeln der auf einem ELM-Speichergerät gespeicherten Daten können Sie ein beliebiges Speichergerät verwenden, das zur Liste der verfügbaren Geräte hinzugefügt wurde und über den benötigten Speicherplatz verfügt.

Bevor Sie beginnen

Fügen Sie die zwei Geräte, die Sie für die gegenseitige Spiegelung verwenden möchten, zum ESM-Gerät hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Speicherpools**.
2. Klicken Sie neben der unteren Tabelle auf **Hinzufügen**.
3. Geben Sie auf der Seite **Speicherpool hinzufügen** die erforderlichen Informationen ein. Klicken Sie dann auf **Hinzufügen**, um das Speichergerät und das Spiegelgerät hinzuzufügen.

   Ein Gerät kann mehreren Pools gleichzeitig zugewiesen sein.

4. Klicken Sie zweimal auf **OK**.

Erneutes Erstellen eines gespiegelten Speicherpools

Wenn die Verbindung zwischen einem gespiegelten Speicherpool und den zugehörigen Speichergeräten getrennt wird, können Sie den Speicherpool mit der Funktion **Erneut erstellen** reparieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Speicherpool**.
2. Zeigen Sie auf die gespiegelten Geräte, für die ein Warnsymbol angezeigt wird.

   Sie werden über eine QuickInfo informiert, dass die ELM-Zuordnung erneut erstellt wird oder dass das gespiegelte Gerät erneut erstellt werden muss.

3. Zum erneuten Erstellen der gespiegelten Geräte klicken Sie auf die Geräte und dann auf **Erneut erstellen**.

Nach Abschluss des Vorgangs werden Sie benachrichtigt, dass die Zuordnung erfolgreich erneut erstellt wurde.

Deaktivieren eines Spiegelgeräts

Wenn Sie ein Gerät nicht mehr als Spiegelgerät für einen Speicherpool verwenden möchten, müssen Sie ein anderes Gerät als Ersatz auswählen oder **Keines** auswählen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das ELM-Gerät aus, auf dem sich der Spiegelspeicherpool zurzeit befindet, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Speicherpools**, wählen Sie dann die gespiegelten Geräte in der Tabelle **Speicherpool** aus, und klicken Sie auf **Bearbeiten**.

3 Führen Sie einen der folgenden Schritte aus:

- Wenn Sie das im Feld **Gespiegeltes Datenspeichergerät** ausgewählte Gerät deaktivieren möchten, klicken Sie auf den Dropdown-Pfeil in diesem Feld. Wählen Sie ein anderes Gerät zum Spiegeln des Datenspeichergeräts aus, oder wählen Sie **Keines** aus.
- Wenn Sie das im Feld **Datenspeichergerät** ausgewählte Gerät deaktivieren möchten, klicken Sie auf den Dropdown-Pfeil in diesem Feld, und wählen Sie ein anderes Gerät als Datenspeichergerät aus.

4 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Wenn das Gerät nicht mehr als Spiegelgerät fungiert, wird es dennoch weiterhin in der Tabelle **Speichergerät** angezeigt.

Einrichten eines externen Datenspeichers

Zum Speichern von ELM-Daten können Sie drei externe Speichertypen einrichten: iSCSI, SAN und DAS. Wenn diese externen Speichertypen mit dem ELM-Gerät verbunden sind, können Sie sie für die Speicherung von Daten vom ELM-Gerät einrichten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Datenspeicher**.

2 Klicken Sie auf die Registerkarte **iSCSI**, **SAN** oder **DAS**, und führen Sie dann die erforderlichen Schritte aus.

3 Klicken Sie auf **Anwenden** oder **OK**.

Hinzufügen eines iSCSI-Geräts

Wenn Sie ein iSCSI-Gerät als ELM-Speicher verwenden möchten, müssen Sie Verbindungen mit dem Gerät konfigurieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Datenspeicher**.

2 Klicken Sie auf der Registerkarte **iSCSI** auf **Hinzufügen**.

3 Geben Sie erforderlichen Informationen ein, und klicken Sie anschließend auf **OK**.

Wenn die Verbindung erfolgreich hergestellt wurde, werden das Gerät und die zugehörigen IQNs zur Liste **iSCSI-Konfiguration** sowie zur Liste **Gerätetyp** auf der Seite **Speichergerät hinzufügen** hinzugefügt (siehe *Hinzufügen eines Speichergeräts*).

Nach Beginn der Speicherung von ELM-Protokollen auf einem IQN kann das iSCSI-Ziel nicht gelöscht werden. Aufgrund dieser Einschränkung müssen Sie darauf achten, auf dem iSCSI-Ziel ausreichend Speicherplatz für den ELM-Speicher einzurichten.

4 Bevor Sie einen IQN als ELM-Speicher verwenden, wählen Sie ihn in der Liste aus, und klicken Sie dann auf **Format**.

5 Zum Überprüfen des Formatierungsstatus klicken Sie auf **Status überprüfen**.

6 Zum Entdecken oder erneuten Entdecken der IQNs klicken Sie auf das iSCSI-Gerät und dann auf **Entdecken**.

Wenn Sie versuchen, einem IQN mehrere Geräte zuzuweisen, kann es zu Datenverlusten kommen.

Formatieren eines SAN-Speichergeräts zum Speichern von ELM-Daten

Wenn im System eine SAN-Karte vorhanden ist, können Sie diese zum Speichern von ELM-Daten verwenden.

Bevor Sie beginnen

Installieren Sie eine SAN-Karte im System (siehe *Installieren des qLogic 2460 SAN-Adapters* in **McAfee ESM** – Einrichtungs- und Installationshandbuch, oder wenden Sie sich an den McAfee-Support).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Datenspeicher**.

2 Klicken Sie auf die Registerkarte **SAN**, und überprüfen Sie dann den Status der erkannten SAN-Volumes.

- **Formatieren erforderlich**: Das Volume muss formatiert werden und wird nicht in der Liste der verfügbaren Volumes auf der Seite **Speichergerät hinzufügen** angezeigt.
- **Formatierung**: Das Volume wird gerade formatiert und wird nicht in der Liste der verfügbaren Volumes angezeigt.
- **Bereit**: Das Volume wurde formatiert und hat ein erkennbares Dateisystem. Diese Volumes können zum Speichern von ELM-Daten verwendet werden.

3 Wenn Sie auf einem nicht formatierten Volume Daten speichern möchten, klicken Sie auf das Volume und dann auf **Format**.

Beim Formatieren eines Volumes werden alle gespeicherten Daten gelöscht.

4 Um zu überprüfen, ob die Formatierung abgeschlossen ist, klicken Sie auf **Aktualisieren**.

Wenn die Formatierung abgeschlossen ist, wird der Status in **Bereit** geändert.

5 Zum Anzeigen der Details eines Volumes unten auf der Seite klicken Sie auf das Volume.

Nun können Sie das formatierte SAN-Volume als Speichergerät für die ELM-Speicherung einrichten.

Zuweisen eines DAS-Geräts zum Speichern von Daten

Sie können verfügbare DAS-Geräte für die Speicherung von ELM-Daten zuweisen.

Bevor Sie beginnen

Richten Sie DAS-Geräte ein.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das ELM-Gerät aus, dem Sie das DAS-Gerät zuweisen möchten, und klicken Sie dann auf das Symbol **Eigenschaften**  .



Bei einem All-in-One-Gerät können Sie das DAS-Gerät dem ESM-Gerät zuweisen, indem Sie das ESM-Gerät auswählen und dann auf das Symbol **Eigenschaften** klicken.

2 Klicken Sie auf **Datenspeicher** und dann auf die Registerkarte **DAS**.

In der Tabelle **DAS** werden die als Speicher verfügbaren Geräte aufgeführt.

3 Klicken Sie in der Tabelle auf eines der Geräte, die nicht zum Speichern von ELM- oder ESM-Daten zugewiesen sind.

4 Klicken Sie auf **Zuweisen** und dann auf der Warnungsseite auf **Ja**.



Ein zugewiesenes Gerät können Sie später nicht ändern.

Das ELM-Gerät wird neu gestartet.

ELM-Redundanz

Sie können Redundanz für die Protokollierung bereitstellen, indem Sie ein ELM-Standby-Gerät zum aktuellen eigenständigen ELM-Gerät im System hinzufügen.

Zum Aktivieren der Redundanz definieren Sie die IP-Adressen und andere Netzwerkinformationen für zwei ELM-Geräte (siehe *Einrichten der ELM-Redundanz*). Das ELM-Standby-Gerät muss über Speichergeräte verfügen, auf denen insgesamt genauso viel Speicherplatz wie auf dem aktiven ELM-Gerät vorhanden ist. Wenn die beiden ELM-Geräte eingerichtet sind, werden ihre Konfigurationen synchronisiert, und die Daten der beiden Geräte werden durch das ELM-Standby-Gerät kontinuierlich synchronisiert.

Beim Arbeiten mit ELM-Redundanz können Sie verschiedene Aktionen ausführen: zwischen Geräten wechseln, Geräte wieder in Betrieb nehmen, anhalten und entfernen sowie den Status von Geräten anzeigen. Alle Aktionen sind auf der Seite **ELM-Eigenschaften** | **ELM-Redundanz** verfügbar.

Wechseln zwischen Geräten

Wenn das primäre ELM-Gerät inaktiv ist oder ersetzt werden muss, wählen Sie **ELM-Geräte wechseln** aus. Das ELM-Standby-Gerät wird aktiv, und alle Protokollierungsgeräte werden ihm vom System zugeordnet. Während des Wechselvorgangs sind Protokollierungs- und Konfigurationsaktionen gesperrt.

Wieder in Betrieb nehmen

Wenn das ELM-Standby-Gerät inaktiv wird und dann wieder aktiviert wird, müssen Sie es wieder in Betrieb nehmen. Wenn keine Änderungen an den Konfigurationsdateien erkannt werden, wird die Redundanz wie zuvor fortgesetzt. Wenn Unterschiede in den Dateien erkannt werden, wird die Redundanz für die Speicherpools ohne Probleme fortgesetzt. Dabei wird jedoch ein Fehlerstatus zurückgegeben, aus dem hervorgeht, dass mindestens ein Pool über eine abweichende Konfiguration verfügt. Diese Pools müssen Sie manuell korrigieren.

Wenn Sie das ELM-Standby-Gerät ersetzen oder erneut konfigurieren, wird dies vom System erkannt, und Sie werden aufgefordert, den Authentifizierungsschlüssel für das Gerät erneut festzulegen. Alle Konfigurationsdateien werden dann vom aktiven ELM-Gerät mit dem ELM-Standby-Gerät synchronisiert, und die Redundanz wird wie zuvor fortgesetzt.

Anhalten

Sie können die Kommunikation mit dem ELM-Standby-Gerät anhalten, wenn das Gerät inaktiv ist oder wird. Die gesamte Kommunikation wird angehalten, und Fehlerbenachrichtigungen für die Redundanz werden maskiert. Wenn das ELM-Standby-Gerät wieder aktiviert wird, führen Sie das Verfahren für die Wiederinbetriebnahme aus.

Deaktivieren der Redundanz auf dem ELM-Gerät

Sie können die ELM-Redundanz deaktivieren, indem Sie die Option **Entfernen** auswählen. Auf dem aktiven ELM-Gerät wird eine Kopie der Redundanzkonfigurationsdateien gespeichert. Wenn diese Sicherungsdatei beim Aktivieren der ELM-Redundanz gefunden wird, werden Sie gefragt, ob Sie die gespeicherten Konfigurationsdateien wiederherstellen möchten.

Anzeigen des Status

Sie können Details zum Status der Datensynchronisierung zwischen dem aktiven ELM-Gerät und dem ELM-Standby-Gerät anzeigen, indem Sie die Option **Status** auswählen.

Einrichten der ELM-Redundanz

Wenn im System ein eigenständiges ELM-Gerät vorhanden ist, können Sie Redundanz für die Protokollierung bereitstellen, indem Sie ein ELM-Standby-Gerät hinzufügen.

Bevor Sie beginnen

Ein eigenständiges ELM-Gerät muss installiert (siehe *McAfee Enterprise Security Manager 9.5.0 – Installationshandbuch*) und zur ESM-Konsole hinzugefügt sein (siehe *Hinzufügen von Geräten zur ESM-Konsole*). Außerdem muss ein ELM-Standby-Gerät installiert sein, das nicht zur Konsole hinzugefügt wurde. Stellen Sie sicher, dass sich auf dem ELM-Standby-Gerät keine Daten befinden. Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten, wenden Sie sich an den McAfee-Support.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Systemnavigationsstruktur auf das ELM-Gerät und dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf der Seite **ELM-Eigenschaften** auf **ELM-Redundanz** und dann auf **Aktivieren**.
3. Geben Sie die IP-Adresse und das Kennwort für das ELM-Standby-Gerät ein, und klicken Sie dann auf **OK**.
4. Klicken Sie auf der Seite **ELM-Eigenschaften** auf **Speicherpools**, und vergewissern Sie sich, dass die Registerkarte **Aktiv** ausgewählt ist.
5. Fügen Sie Speichergeräte zum aktiven ELM-Gerät hinzu (siehe *Hinzufügen eines Speichergeräts für die Verknüpfung mit einem Speicherpool*).
6. Klicken Sie auf die Registerkarte **Standby**, und fügen Sie dann Speichergeräte hinzu, auf denen insgesamt genauso viel Speicherplatz wie auf dem aktiven ELM-Gerät vorhanden ist.
7. Fügen Sie zu jedem ELM-Gerät mindestens einen Speicherpool hinzu (siehe *Hinzufügen oder Bearbeiten eines Speicherpools*).

Nun werden die Konfigurationen der beiden ELM-Geräte synchronisiert, und die Daten der beiden Geräte werden durch das ELM-Standby-Gerät kontinuierlich synchronisiert.

Verwalten der ELM-Komprimierung

Komprimieren Sie die auf dem ELM-Gerät eingehenden Daten, um Speicherplatz zu sparen oder mehr Protokolle pro Sekunde zu verarbeiten.

Die drei Optionen lauten **Niedrig** (Standard), **Mittel** und **Hoch**. In dieser Tabelle werden Details zu den einzelnen Stufen angezeigt.

Stufe	Komprimierungsrate	Prozentsatz der maximalen Komprimierung	Prozentsatz der maximal pro Sekunde verarbeiteten Protokolle
Niedrig	14:1	72%	100%
Mittel	17:1	87%	75%
Hoch	20:1	100%	50%

Die tatsächlichen Komprimierungsraten fallen je nach Inhalt der Protokolle unterschiedlich aus.

- Wenn es Ihnen wichtiger ist, Speicherplatz zu sparen, während die Anzahl der pro Sekunde verarbeiteten Protokolle von geringerer Bedeutung ist, wählen Sie hohe Komprimierung aus.
- Wenn es Ihnen wichtiger ist, mehr Protokolle pro Sekunde zu verarbeiten, als Speicherplatz zu sparen, wählen Sie niedrige Komprimierung aus.

Festlegen der ELM-Komprimierung

Wählen Sie die Komprimierungsstufe für die auf dem ELM-Gerät eingehenden Daten aus, um Speicherplatz zu sparen oder mehr Protokolle zu verarbeiten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **ELM-Konfiguration** | **Komprimierung**.
2. Wählen Sie die ELM-Komprimierungsstufe aus, und klicken Sie dann auf **OK**.

Nach der Aktualisierung der Stufe werden Sie benachrichtigt.

Anzeigen der Ergebnisse einer Suche oder Integritätsprüfung

Nach Abschluss eines Such- oder Integritätsprüfungsauftrags können Sie die Ergebnisse anzeigen.

Bevor Sie beginnen

Führen Sie einen Such- oder Integritätsprüfungsauftrag aus, der zu Ergebnissen führt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus.
2. Klicken Sie auf **Daten**, und wählen Sie dann die Registerkarte **Protokolle und Dateien durchsuchen** oder **Integritätsprüfung** aus.
3. Heben Sie in der Tabelle **Suchergebnisse** den anzuzeigenden Auftrag hervor, und klicken Sie dann auf **Ansicht**.

Auf der Seite **ELM-Suchergebnisse** werden die Ergebnisse des Auftrags angezeigt.

Wenn Sie mehrere zusätzliche VM-Laufwerke gleichzeitig vom ESM-Gerät entfernen, gehen möglicherweise alle ELM-Suchen verloren. Vermeiden Sie den Verlust der Ergebnisse, indem Sie die ELM-Suchergebnisse exportieren.

Sichern und Wiederherstellen von ELM

Bei einem Systemfehler oder Datenverlust müssen Sie die aktuellen Einstellungen auf ELM-Geräten sichern. Alle Konfigurationseinstellungen, einschließlich der Datenbank für die ELM-Protokollierung, werden gesichert. Die eigentlichen auf dem ELM-Gerät gespeicherten Protokolle werden nicht gesichert.

Es wird empfohlen, die Geräte, auf denen die Protokolldaten des ELM-Geräts gespeichert werden, und die ELM-Verwaltungsdatenbank zu spiegeln. Mit der Spiegelung können Sie Echtzeitprotokolldaten sichern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus.

2 Vergewissern Sie sich, dass **ELM-Informationen** ausgewählt ist, und klicken Sie dann auf **Sichern und wiederherstellen**.

3 Führen Sie einen der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Sofortiges Sichern von ELM	Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **Jetzt sichern**.
Automatisches Sichern der ELM-Einstellungen	Wählen Sie die Häufigkeit aus, und geben Sie die Informationen ein.
Sofortiges Wiederherstellen der Sicherung	Klicken Sie auf **Sicherung jetzt wiederherstellen**. Die ELM-Datenbank wird mit den Einstellungen aus einer vorherigen Sicherung wiederhergestellt.

Wiederherstellen der ELM-Verwaltungsdatenbank und der Protokolldaten

Zum Ersetzen eines ELM-Geräts stellen Sie die Verwaltungsdatenbank und die Protokolldaten auf dem neuen ELM-Gerät wieder her. Dazu müssen Sie die Datenbank und die Protokolldaten spiegeln.

Erstellen Sie beim Wiederherstellen der Daten von einem alten ELM-Gerät auf einem neuen ELM-Gerät nicht mit dem Assistenten **Gerät hinzufügen** ein neues ELM-Gerät.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** für das zu ersetzende ELM-Gerät aus.

Auf einer Warnungsseite werden Sie informiert, dass das ELM-Gerät vom System nicht gefunden wurde.

2 Schließen Sie die Warnungsseite, und klicken Sie dann auf **Verbindung**.

3 Geben Sie die IP-Adresse für das neue ELM-Gerät ein, und klicken Sie dann auf **Schlüsselverwaltung** | **Authentifizierungsschlüssel für Gerät festlegen**.

Sie werden informiert, wenn der Schlüssel für das neue Gerät erfolgreich festgelegt wurde.

4 Geben Sie das Kennwort für das neue Gerät ein, und klicken Sie dann auf **Weiter**.

5 Klicken Sie auf **ELM-Informationen** | **Sichern und wiederherstellen** | **ELM wiederherstellen**.

6 Synchronisieren Sie die einzelnen auf dem ELM-Gerät protokollierten Geräte erneut, indem Sie für jedes Gerät auf **ELM synchronisieren** auf der Seite **Eigenschaften** | **Konfiguration** klicken.

Die Verwaltungsdatenbank und der ELM-Datenspeicher werden auf dem neuen ELM-Gerät wiederhergestellt. Dieser Vorgang kann mehrere Stunden dauern.

Ermöglichen schnellerer ELM-Suchvorgänge

Mit der Volltextindizierung können ELM-Protokolle indiziert werden. Wenn die Funktion aktiviert ist, wird die ELM-Suche beschleunigt, da weniger Dateien durchsucht werden müssen.

Bevor Sie beginnen

Definieren Sie das Speichergerät und den Speicherplatz, den Sie der Indizierung zuordnen möchten. Wie viele ELM-Protokolle indiziert werden können, hängt davon ab, wie viel Speicherplatz Sie der Indizierung zuordnen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **ELM-Konfiguration** | **Volltextindex**.

2 Wählen Sie auf der Seite **Speicherort der Volltextindizierung auswählen** die erforderlichen Optionen aus.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Anzeigen der Verwendung des ELM-Speichers

Sie können die Verwendung des Speichers auf dem ELM-Gerät anzeigen, um Entscheidungen bezüglich der Speicherplatzzuordnung auf dem Gerät zu treffen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **ELM-Verwaltung**.

2 Klicken Sie auf **Verwendung anzeigen**.

Die Seite **Verwendungsstatistik** wird geöffnet. Hier wird die Statistik für das Speichergerät und die Speicherpools auf dem ELM-Gerät angezeigt.

3 Klicken Sie auf **OK**.

Migrieren der ELM-Datenbank

In der ELM-Verwaltungsdatenbank werden die Datensätze gespeichert, in denen die an das ELM-Gerät gesendeten Protokolle verfolgt werden. Wie viel Speicherplatz auf dem ELM-Gerät zum Speichern der Verwaltungsdatenbank verfügbar ist, hängt vom Modell ab.

Beim anfänglichen Hinzufügen des Geräts wird überprüft, ob genügend Speicherplatz für die Datensätze vorhanden ist. Wenn dies nicht der Fall ist, werden Sie aufgefordert, einen alternativen Speicherort für die Verwaltungsdatenbank zu definieren. Wenn auf dem Gerät genügend Speicherplatz vorhanden ist und Sie die Datenbank dennoch an einem anderen Speicherort speichern möchten, können Sie diesen Speicherort auf der Seite **ELM-Eigenschaften** mit der Option **Datenbank migrieren** einrichten.

Die Option **Datenbank migrieren** können Sie jederzeit verwenden. Wenn die Verwaltungsdatenbank bei der Migration jedoch bereits Datensätze enthält, wird die ELM-Sitzung abhängig von der Anzahl der enthaltenen Datensätze bis zum Abschluss der Migration mehrere Stunden lang angehalten. Es wird empfohlen, diesen alternativen Speicherort beim anfänglichen Einrichten des ELM-Geräts zu definieren.

Definieren eines alternativen Speicherorts

Wenn Sie die ELM-Verwaltungsdatenbank an einem Speicherort außerhalb des ELM-Geräts speichern möchten, müssen Sie den alternativen Speicherort definieren. Außerdem können Sie ein zweites Gerät zum Spiegeln der gespeicherten Daten auswählen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **ELM-Konfiguration** | **Datenbank migrieren**.
2. Wählen Sie das Speichergerät und ein gespiegeltes Gerät aus.
3. Klicken Sie auf **OK**.

Ersetzen einer gespiegelten ELM-Verwaltungsdatenbank

Wenn auf einem Speichergerät für eine gespiegelte Verwaltungsdatenbank ein Problem auftritt, müssen Sie das Gerät möglicherweise ersetzen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das ELM-Gerät mit dem Speichergerät für die Verwaltungsdatenbank aus, auf dem das Problem auftritt. Klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **ELM-Konfiguration**, und wählen Sie dann **Datenbank migrieren** aus.
3. Wählen Sie im Feld **Datenspeichergeräte** das in der Dropdown-Liste **Gespiegeltes Datenspeichergerät** aufgeführte Gerät aus.
4. Wählen Sie im Feld **Gespiegeltes Datenspeichergerät** ein neues Gerät aus, oder wählen Sie **Keines** aus, um die Spiegelung anzuhalten.



Wenn das gewünschte Gerät in der Dropdown-Liste nicht aufgeführt wird, fügen Sie das Gerät zuerst zur Tabelle **Speichergerät** hinzu.

Abrufen von ELM-Daten

Zum Abrufen von Daten vom ELM-Gerät müssen Sie auf der Seite **Daten** Such- und Integritätsprüfungsaufträge erstellen.

Bei einem Integritätsprüfungsauftrag wird überprüft, ob die von Ihnen angegebenen Dateien seit der ursprünglichen Speicherung geändert wurden. Dies kann eine Warnung vor nicht autorisierten Änderungen an kritischen System- oder Inhaltsdateien sein. Aus den Ergebnissen der Überprüfung geht hervor, welche Dateien geändert wurden. Wenn keine der Dateien geändert wurde, werden Sie benachrichtigt, dass die Überprüfung erfolgreich ausgeführt wurde.

Sie können insgesamt 50 Suchvorgänge und Integritätsprüfungsaufträge gleichzeitig ausführen. Bei mehr als 50 dieser Aufträge im System werden Sie informiert, dass die Suche nicht ausgeführt werden kann. Sie können im System vorhandene Suchvorgänge löschen, damit die neue Suche ausgeführt

werden kann. Wenn keine Suchvorgänge vorhanden sind, löscht der Systemadministrator vorhandene von anderen Benutzern initiierte Suchvorgänge oder Integritätsprüfungsaufträge, damit Ihre Suche ausgeführt werden kann.

Eine initiierte Suche wird ausgeführt, bis sie abgeschlossen ist oder eines der festgelegten Limits erreicht ist. Dies gilt auch, wenn Sie die Seite **Daten** schließen. Sie können zu diesem Bildschirm zurückkehren, um den Status der Suche zu überprüfen, der in der Tabelle **Suchergebnisse** angezeigt wird.

Erstellen eines Suchauftrags

Zum Durchsuchen des ELM-Geräts nach Dateien, die Ihren Kriterien entsprechen, müssen Sie auf der Seite **Daten** einen Suchauftrag definieren. Keines der Felder auf diesem Bildschirm ist erforderlich. Je genauer Sie jedoch die Suche definieren, umso wahrscheinlicher können Sie die benötigten Daten in kürzestmöglicher Zeit abrufen.

Die Geschwindigkeit der ELM-Suche wurde in Version 9.2.0 erhöht. Damit diese Steigerung beim Durchführen eines Upgrades von Versionen vor 9.2.0 auf Versionen nach 9.2.0 wirksam wird, müssen Sie das FTI-System (Full-Text Indexer, Volltextindizierung) aktivieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Daten**.
2. Geben Sie auf der Registerkarte **Protokolle und Dateien durchsuchen** die erforderlichen Informationen ein, und klicken Sie dann auf **Suchen**.

Erstellen eines Integritätsprüfungsauftrags

Sie können überprüfen, ob Dateien seit der ursprünglichen Speicherung geändert wurden. Dazu erstellen Sie auf der Seite **Daten** einen Integritätsprüfungsauftrag. Keines der Felder auf der Registerkarte **Integritätsprüfung** ist erforderlich. Je genauer Sie jedoch die Suche definieren, umso wahrscheinlicher können Sie die Integrität der benötigten Daten in kürzestmöglicher Zeit überprüfen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ELM-Eigenschaften** aus, und klicken Sie dann auf **Daten**.
2. Klicken Sie auf die Registerkarte **Integritätsprüfung**, wählen Sie die erforderlichen Optionen aus, und klicken Sie dann auf **Suchen**.

Einstellungen für Advanced Correlation Engine (ACE)

Mit McAfee Advanced Correlation Engine (ACE) werden anhand einer regel- und risikobasierten Logik Bedrohungsereignisse in Echtzeit identifiziert und bewertet.

Sie geben an, worauf Sie Wert legen (Benutzer oder Gruppen, Anwendungen, bestimmte Server oder Subnetze), und werden von ACE gewarnt, wenn die jeweilige Ressource bedroht ist. Für Audit-Listen und die Wiedergabe des Verlaufs werden forensische Funktionen, Compliance-Regeln und Regeloptimierung unterstützt.

Sie können für ACE den Echtzeitmodus oder den historischen Modus konfigurieren:

- **Echtzeitmodus**: Ereignisse werden bei der Erfassung zur unmittelbaren Erkennung von Bedrohungen und Risiken analysiert.
- **Historischer Modus**: Die verfügbaren Daten werden über eines oder beide Korrelationsmodule wiedergegeben, um historische Bedrohungen und Risiken zu erkennen. Wenn von ACE neue Zero-Day-Angriffe erkannt werden, wird ermittelt, ob das Unternehmen dem jeweiligen Angriff in der Vergangenheit ausgesetzt war. So können *Sub-Zero-Day*-Bedrohungen erkannt werden.

Mit den zwei bereitgestellten dedizierten Korrelationsmodulen stellen ACE-Geräte eine Ergänzung zu den vorhandenen Ereigniskorrelationsfunktionen für ESM dar. Konfigurieren Sie die einzelnen ACE-Geräte mit eigenen Einstellungen für Richtlinien, Verbindungen, Ereignisse und Protokollabruf und eigenen Risiko-Managern.

- **Risikokorrelation**: Hierbei wird mithilfe einer regellosen Korrelation ein Risikofaktor generiert. Bei der regelbasierten Korrelation werden nur bekannte Bedrohungsmuster erkannt. Die Signaturen müssen ständig optimiert und aktualisiert werden, damit die Korrelation effektiv ist. Bei der regellosen Korrelation werden Erkennungssignaturen durch eine einmalige Konfiguration ersetzt: Geben Sie an, welche Bereiche für das Unternehmen wichtig sind (beispielsweise bestimmte Dienste oder Anwendungen, Benutzergruppen oder Datentypen). Bei der **Risikokorrelation** werden dann alle Aktivitäten im Zusammenhang mit diesen Elementen verfolgt. Dadurch entsteht ein dynamischer Risikofaktor, der abhängig von den Echtzeitaktivitäten steigt oder sinkt.

  Wenn ein Risikofaktor einen bestimmten Schwellenwert überschreitet, wird in ACE ein Ereignis generiert, und Sie werden vor steigenden Bedrohungsbedingungen gewarnt. Alternativ kann das Ereignis vom herkömmlichen regelbasierten Korrelationsmodul als Bedingung für einen größeren Vorfall verwendet werden. In ACE wird eine Audit-Liste mit allen Risikofaktoren geführt, die die vollständige Analyse und Untersuchung von Bedrohungsbedingungen im Zeitverlauf ermöglicht.

- Bei der **regelbasierten Korrelation** werden Bedrohungen mithilfe einer regelbasierten Ereigniskorrelation erkannt und die erfassten Informationen in Echtzeit analysiert. Alle Protokolle, Ereignisse und Netzwerkflüsse werden in ACE korreliert – zusammen mit Informationen zum Kontext wie beispielsweise Identitäten, Rollen, Schwachstellen usw. –, um Muster zu erkennen, die auf eine größere Bedrohung hinweisen.

  Von Event Receiver-Geräten wird netzwerkweite regelbasierte Korrelation unterstützt. ACE dient als Ergänzung dieser Funktion und bietet eine dedizierte Verarbeitungsressource, mit der umfangreichere Datenmengen korreliert werden können, entweder als Ergänzung für vorhandene Korrelationsberichte oder durch vollständige Auslagerung der Daten.

Konfigurieren Sie die einzelnen ACE-Geräte mit eigenen Einstellungen für Richtlinien, Verbindungen, Ereignisse und Protokollabruf und eigenen Risiko-Managern.

Auswählen des ACE-Datentyps

Auf dem ESM-Gerät werden Ereignis- und Flussdaten erfasst. Wählen Sie aus, welche Daten an ACE gesendet werden sollen. Standardmäßig werden nur Ereignisdaten gesendet.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ACE-Eigenschaften** aus, und klicken Sie dann auf **ACE-Konfiguration**.
2. Klicken Sie auf **Daten**, und wählen Sie dann **Ereignisdaten** und/oder **Flussdaten** aus.
3. Klicken Sie auf **OK**.

Hinzufügen eines Korrelations-Managers

Zum Verwenden der Regel- oder Risikokorrelation müssen Sie Regel- oder Risikokorrelations-Manager hinzufügen.

Bevor Sie beginnen

In ESM muss ein ACE-Gerät vorhanden sein (siehe *Hinzufügen von Geräten zur ESM-Konsole*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ACE-Eigenschaften** aus, und klicken Sie dann auf **Korrelationsverwaltung**.
2. Wählen Sie den Typ des zu erstellenden Managers aus, und klicken Sie dann auf **OK**.
3. Wenn Sie **Regelkorrelation** ausgewählt haben, füllen Sie die Registerkarten **Hauptbildschirm** und **Filter** aus. Wenn Sie **Risikokorrelation** ausgewählt haben, füllen Sie die Registerkarten **Hauptbildschirm**, **Felder**, **Schwellenwerte** und **Filter** aus.
4. Klicken Sie auf **Fertig stellen**.

Hinzufügen eines Risikokorrelations-Managers

Sie müssen für die Berechnung der Risikostufen für die festgelegten Felder Manager hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ACE-Eigenschaften** aus, und klicken Sie dann auf **Risikokorrelations-Verwaltung**.
2. Klicken Sie auf **Hinzufügen**, und geben Sie dann auf den einzelnen Registerkarten die erforderlichen Informationen ein.
3. Klicken Sie auf **Fertig stellen** und dann auf **Schreiben**, um die Manager in das Gerät zu schreiben.

Hinzufügen des Faktors für Risikokorrelation

Sie müssen Bedingungsanweisungen hinzufügen, mit denen ein Faktor für ein Zielfeld zugewiesen wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ACE-Eigenschaften** aus, und klicken Sie dann auf **Risikokorrelations-Bewertung**.
2. Klicken Sie auf **Hinzufügen**, und geben Sie dann die erforderlichen Informationen ein.
3. Klicken Sie auf **OK**.

Verwenden der historischen Korrelation

Mit der Option Historische Korrelation können Sie vergangene Ereignisse korrelieren.

Wenn eine neue Schwachstelle entdeckt wird, ist es wichtig, dass Sie die historischen Ereignisse überprüfen, um herauszufinden, ob die Schwachstelle in der Vergangenheit ausgenutzt wurde. Mithilfe der einfachen ACE-Funktion für Netzwerkwiederholungen können historische Ereignisse durch das

regellose Korrelationsmodul **Risikokorrelation** wiedergegeben werden. Dabei können Sie anhand des auf Standardregeln basierenden Ereigniskorrelationsmoduls historische Ereignisse im Hinblick auf gegenwärtige Bedrohungen untersuchen. Dies kann in den folgenden Situationen hilfreich sein:

- Bei der Auslösung bestimmter Ereignisse war die Korrelation nicht eingerichtet, und Sie stellen fest, dass Sie durch die Korrelation wertvolle Informationen erhalten hätten.
- Sie richten eine neue Korrelation ein, die auf in der Vergangenheit ausgelösten Ereignissen basiert. Dabei möchten Sie die neue Korrelation testen, um sicherzustellen, dass Sie die gewünschten Ergebnisse erhalten.

Beachten Sie beim Einsatz der historischen Korrelation Folgendes:

- Die Echtzeitkorrelation wird angehalten, bis Sie die historische Korrelation deaktivieren.
- Die Risikoverteilung wird durch die Ereignisaggregation verzerrt.
- Wenn Sie den Risiko-Manager wieder in die Risikokorrelation in Echtzeit verschieben, müssen Sie die Schwellenwerte optimieren.

Führen Sie die folgenden Schritte zum Einrichten und Ausführen der historischen Korrelation aus:

1 Fügen Sie einen Filter für historische Korrelation hinzu.

2 Führen Sie eine historische Korrelation aus.

3 Laden Sie die korrelierten historischen Ereignisse herunter, und zeigen Sie sie an.

Hinzufügen und Ausführen einer historischen Korrelation

Richten Sie zum Korrelieren vergangener Ereignisse einen Filter für historische Korrelation ein, und führen Sie dann die Korrelation aus.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ACE-Eigenschaften** aus, und klicken Sie dann auf **Historisch**.

2 Klicken Sie auf **Hinzufügen**, geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

3 Wählen Sie **Historische Korrelation aktivieren** aus, und klicken Sie dann auf **Anwenden**.

Die Echtzeitkorrelation wird angehalten, bis Sie die historische Korrelation deaktivieren.

4 Wählen Sie die auszuführenden Filter aus, und klicken Sie dann auf **Jetzt ausführen**.

Die Ereignisse werden von ESM überprüft, die Filter werden angewendet, und die entsprechenden Ereignisse werden in Paketen zusammengefasst.

Herunterladen und Anzeigen der Ereignisse der historischen Korrelation

Wenn Sie die historische Korrelation ausgeführt haben, können Sie die dabei generierten Ereignisse herunterladen und anzeigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ACE-Eigenschaften** aus, und klicken Sie dann auf **Ereignisse und Protokolle | Ereignisse abrufen**.

   Die Ereignisse, die sich beim Ausführen der historischen Korrelation ergeben haben, werden in ESM heruntergeladen.

2 Schließen Sie **ACE-Eigenschaften**.

3 So zeigen Sie die Daten an:

   a Wählen Sie in der Systemnavigationsstruktur das ACE-Gerät aus, für das Sie die historischen Daten abgerufen haben.

   b Wählen Sie auf der Ansichtssymbolleiste in der Dropdown-Liste für Zeiträume den Zeitraum aus, den Sie beim Einrichten der Abfrage angegeben haben.

Die Ergebnisse der Abfrage werden im Ansichtsbereich angezeigt.

Einstellungen für Application Data Monitor (ADM)

Mit McAfee Application Data Monitor (ADM) wird die gesamte Verwendung vertraulicher Daten im Netzwerk verfolgt. Dabei werden die zugrunde liegenden Protokolle, die Sitzungsintegrität und der Anwendungsinhalt analysiert.

Wenn eine Verletzung in ADM erkannt wird, bleiben alle Details der jeweiligen Anwendungssitzung erhalten und können bei Reaktionen auf Vorfälle und für forensische Funktionen oder für Anforderungen in Bezug auf Compliance-Audits verwendet werden. Gleichzeitig erhalten Sie mit ADM Einblicke in Bedrohungen, die als legitime Anwendungen maskiert sind.

Mit ADM können Sie erkennen, wenn vertrauliche Informationen in E-Mail-Anhängen, bei Instant Messaging, Dateiübertragungen, HTTP POST-Vorgängen oder in anderen Anwendungen übertragen werden. Passen Sie die Erkennungsfunktionen von ADM an, indem Sie eigene Wörterbücher für vertrauliche Informationen definieren. Die vertraulichen Datentypen werden dann von ADM erkannt, die entsprechenden Mitarbeiter werden gewarnt, und der Verstoß wird protokolliert, sodass eine Audit-Liste geführt wird.

Dabei werden in ADM Anomalien in den folgenden Anwendungsprotokollen überwacht, decodiert und erkannt:

- Dateiübertragung: FTP, HTTP, SSL (nur Setup und Zertifikate)
- E-Mail: SMTP, POP3, NNTP, MAPI
- Chat: MSN, AIM/Oscar, Yahoo, Jabber, IRC
- Web-Mail: Hotmail, Hotmail DeltaSync, Yahoo Mail, AOL Mail, Gmail
- P2P: Gnutella, BitTorrent
- Shell: SSH (nur Entdeckung), Telnet

Sie können für ADM Regelausdrücke verwenden, die anhand des überwachten Datenverkehrs getestet werden. Dabei werden für jede ausgelöste Regel Datensätze in die Ereignistabelle der Datenbank eingefügt. Das Paket, durch das die Regel ausgelöst wurde, wird im Paketfeld der Ereignistabelle gespeichert. Außerdem werden für jede ausgelöste Regel Metadaten auf Anwendungsebene zu der dbsession-Tabelle und der Abfragetabelle der Datenbank hinzugefügt. Eine Textdarstellung des Protokoll-Stacks wird im Paketfeld der Abfragetabelle gespeichert.

In ADM können die folgenden Ereignistypen generiert werden:

- **Metadaten**: In ADM wird für jede Transaktion im Netzwerk ein Metadatenereignis generiert, in dem Details zu Adressen, Protokoll, Dateityp und Dateiname enthalten sind. Die Metadatenereignisse werden in die Abfragetabelle eingefügt und mithilfe der Sitzungstabelle gruppiert. Wenn beispielsweise in einer FTP-Sitzung drei Dateien übertragen wurden, werden diese von ADM zusammen gruppiert.
- **Protokollanomalie**: Protokollanomalien sind fest in die Protokollmodule codiert. Dazu gehören Ereignisse wie beispielsweise ein TCP-Paket (Transmission Control Protocol), das zu kurz ist, um einen gültigen Header zu enthalten, und die Rückgabe eines ungültigen Antwortcodes durch einen SMTP-Server (Simple Mail Transfer Protocol). Ereignisse im Zusammenhang mit Protokollanomalien sind selten und werden in der Ereignistabelle abgelegt.
- **Regelauslöser**: Regelauslöseereignisse werden generiert, wenn durch Regelausdrücke Anomalien in den von ICE (Internet Communications Engine) generierten Metadaten erkannt werden. Eine Anomalie liegt beispielsweise vor, wenn ein Protokoll außerhalb der gewohnten Zeiten verwendet wird oder auf einem SMTP-Server unerwartet über FTP kommuniziert wird. Regelauslöseereignisse müssen selten sein und werden in der Ereignistabelle abgelegt.

Die Ereignistabelle enthält einen Datensatz für jedes erkannte Protokollanomalie- oder Regelauslöseereignis. Die Ereignisdatensätze sind über die Sitzungs-ID mit der Sitzungstabelle und der Abfragetabelle verknüpft. Dort finden Sie weitere Details zu den Netzwerkübertragungen (Metadatenereignissen), durch die das Ereignis ausgelöst wurde. Jedes Ereignis ist außerdem mit der Pakettabelle verknüpft, in der die unformatierten Paketdaten für das Paket, durch das das Ereignis ausgelöst wurde, zur Verfügung stehen.

Die Sitzungstabelle enthält einen Datensatz für jede Gruppe zusammengehörender Übertragungen im Netzwerk (z. B. eine Gruppe von FTP-Dateiübertragungen in der gleichen Sitzung). Die Sitzungsdatensätze sind über die Sitzungs-ID mit der Abfragetabelle verknüpft, in der Sie weitere Details zu den einzelnen Netzwerkübertragungen (Metadatenereignissen) finden. Darüber hinaus ist für Übertragungen innerhalb der Sitzung, die eine Protokollanomalie verursachen oder eine Regel auslösen, eine Verknüpfung mit der Ereignistabelle vorhanden.

Die Abfragetabelle enthält einen Datensatz für jedes Metadatenereignis (Inhaltsübertragungen im Netzwerk). Die Abfragedatensätze sind über die Sitzungs-ID mit der Sitzungstabelle verknüpft. Wenn durch die mit dem Datensatz verbundene Netzwerkübertragung eine Protokollanomalie oder Regel ausgelöst wird, ist eine Verknüpfung mit der Ereignistabelle vorhanden. Außerdem gibt es eine Verknüpfung mit der Pakettabelle. Dabei wird das Textfeld verwendet, in dem sich eine Textdarstellung des vollständigen Protokolls oder Inhalts-Stacks befindet.

Festlegen der ADM-Zeitzone

Das ADM-Gerät ist auf GMT festgelegt, während im ADM-Code erwartet wird, dass das Gerät auf Ihre Zeitzone festgelegt ist. Daher werden zeitabhängige Regeln so ausgelöst, als befänden Sie sich in der Zeitzone GMT. Dies ist möglicherweise nicht der Zeitpunkt, den Sie erwartet haben.

Sie können das ADM-Gerät auf die erwartete Zeitzone festlegen. Diese Einstellung wird dann beim Testen der Regeln berücksichtigt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ADM-Eigenschaften** aus, und klicken Sie dann auf **ADM-Konfiguration**.
2. Klicken Sie auf **Zeitzone**, und wählen Sie die Zeitzone aus.
3. Klicken Sie auf **OK**.

Anzeigen des Kennworts in der Sitzungsanzeige

In der **Sitzungsanzeige** können Sie die Details der letzten 25.000 ADM-Abfragen in einer Sitzung anzeigen. Die Regeln für einige der Ereignisse beziehen sich möglicherweise auf Kennwörter. Sie können auswählen, ob die Kennwörter in der **Sitzungsanzeige** angezeigt werden sollen. Standardmäßig werden Kennwörter nicht angezeigt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **ADM-Eigenschaften** aus, und klicken Sie dann auf **ADM-Konfiguration**.

   Für die Option **Kennwörter** ist der Protokollierungsstatus **Aus** angegeben.

2 Klicken Sie auf **Kennwörter**, wählen Sie **Kennwortprotokollierung aktivieren** aus, und klicken Sie dann auf **OK**.

   Der Befehl wird ausgeführt, und Sie werden informiert, wenn er abgeschlossen ist.

Für die Option **Kennwörter** ist jetzt der Protokollierungsstatus **An** angegeben.

Wörterbücher für Application Data Monitor (ADM)

Verwenden Sie beim Schreiben von ADM-Regeln Wörterbücher, mit denen im Netzwerk aufgezeichnete Schlüssel in einen definierten Wert übersetzt werden. Sie können auch Schlüssel ohne Wert auflisten, für die standardmäßig der boolesche Wert wahr verwendet wird, wenn die Schlüssel vorhanden sind.

Mithilfe von ADM-Wörterbüchern können Sie schnell die Schlüssel einer Datei angeben und müssen nicht für jedes Wort eine eigene Regel schreiben. Richten Sie beispielsweise eine Regel ein, um E-Mails auszuwählen, die bestimmte Wörter enthalten, stellen Sie ein Wörterbuch mit unanständigen Wörtern zusammen, und importieren Sie das Wörterbuch. Sie können eine Regel wie die folgende erstellen, um auf E-Mails zu überprüfen, die ein Wort aus dem Wörterbuch enthalten:

```
protocol == email && naughtyWords[objcontent]
```

Beim Schreiben von Regeln mit dem ADM-Regel-Editor können Sie das Wörterbuch auswählen, auf das Sie in der Regel verweisen möchten.



Wörterbücher unterstützen mehrere Millionen von Einträgen.

Beim Hinzufügen eines Wörterbuchs zu einer Regel müssen Sie die folgenden Schritte ausführen:

1 Einrichten und Speichern eines Wörterbuchs, in dem die Schlüssel und gegebenenfalls die Werte aufgeführt sind

2 Verwalten des Wörterbuchs in ESM

3 Zuweisen des Wörterbuchs zu einer Regel

Einrichten eines ADM-Wörterbuchs

Ein Wörterbuch ist eine Klartextdatei mit einem Eintrag pro Zeile. Es gibt ein- und zweispaltige Wörterbücher. Zweispaltige Wörterbücher enthalten einen Schlüssel und einen Wert.

Für die Schlüssel sind die Typen IPv4, MAC, Zahl, Regulärer Ausdruck und Zeichenfolge möglich. Für die Werte sind die Typen Boolescher Wert, IPv4, IPv6, MAC, Zahl und Zeichenfolge möglich. Ein Wert ist optional und wird standardmäßig auf den booleschen Wert Wahr festgelegt, wenn er nicht vorhanden ist.

Werte in einem ein- oder zweispaltigen Wörterbuch müssen einem der unterstützten ADM-Typen entsprechen: Zeichenfolge, Regulärer Ausdruck, Zahl, IPv4, IPv6 oder MAC. Für ADM-Wörterbücher gelten die folgenden Formatierungsrichtlinien:

Typ	Syntaxregeln	Beispiele	Übereinstimmender Inhalt
Zeichenfolge	• Zeichenfolgen müssen in doppelte Anführungszeichen eingeschlossen sein. • Für Anführungszeichen innerhalb einer Zeichenfolge müssen Sie vor jedem Fragezeichen einen umgekehrten Schrägstrich als Escape-Zeichen verwenden.	"Ungültiger Inhalt" "Er sagte \"Ungültiger Inhalt \""	Ungültiger Inhalt Er sagte "Ungültiger Inhalt"
Regulärer Ausdruck	• Reguläre Ausdrücke werden in einzelne Schrägstriche eingeschlossen. • Für Schrägstriche und reservierte Zeichen für reguläre Ausdrücke innerhalb des regulären Ausdrucks müssen Sie einen umgekehrten Schrägstrich als Escape-Zeichen verwenden.	/[Aa]pple/ /Apple/i / [0-9]{1,3}\.[0-9]{1,3}\.[0-9]\.[0-9]/ /1\/2 von allen/	Apple oder apple Apple oder apple IP-Adressen: 1.1.1.1 127.0.0.1 1/2 von allen
Zahlen	• Dezimalwerte (0 – 9) • Hexadezimalwerte (0x0-9a-f) • Oktalwerte (0 – 7)	Dezimalwert Hexadezimalwert Oktalwert	123 0x12ab 0127
Boolesche Werte	• Kann wahr oder falsch sein. • Kleinschreibung	Boolesche Literalwerte	wahr falsch
IPv4	• Kann in standardmäßiger Dotted Quad-Notation geschrieben sein. • Kann in CIDR-Schreibweise geschrieben sein. • Kann im langen Format mit vollständigen Masken geschrieben sein.	192.168.1.1 192.168.1.0/24 192.168.1.0/255.255.255.0	192.168.1.1 192.168.1.[0 – 255] 192.168.1.[0 – 255]

Die folgenden Aussagen treffen auf Wörterbücher zu:

- Listen (mehrere durch Kommas getrennte Werte, die in eckige Klammern eingeschlossen sind) sind in Wörterbüchern nicht zulässig.

- Eine Spalte darf nur aus einem einzigen unterstützten ADM-Typ bestehen. Dies bedeutet, dass Sie nicht in einer einzigen ADM-Wörterbuchdatei verschiedene Typen (Zeichenfolgen, reguläre Ausdrücke, IPv4) beliebig kombinieren können.
- Wörterbücher können Kommentare enthalten. Alle Zeilen, die mit dem Pfundzeichen (#) beginnen, werden in einem ADM-Wörterbuch als Kommentar betrachtet.
- Namen können nur aus alphanumerischen Zeichen und Unterstrichen bestehen und dürfen maximal 20 Zeichen enthalten.
- Listen werden in Wörterbüchern nicht unterstützt.
- Vor ADM 8.5.0 mussten Sie Wörterbücher außerhalb von ESM mit einem Text-Editor Ihrer Wahl bearbeiten oder erstellen. Wörterbücher können über ESM importiert oder exportiert werden, sodass Sie ADM-Wörterbücher leichter ändern oder erstellen können.

Beispiele für ADM-Wörterbücher

Sie können mit dem ADM-Modul Objektinhalte oder beliebige andere Messgrößen oder Eigenschaften mit einem einspaltigen Wörterbuch anhand des Kriteriums wahr oder falsch (ist im Wörterbuch vorhanden oder nicht vorhanden) vergleichen.

Tabelle 3-25 Einspaltiges Wörterbuch, Beispiele

Typ des Wörterbuchs	Beispiel
Wörterbuch für Zeichenfolgen mit allgemeinen Spam-Wörtern	"Cialis" "cialis" "Viagra" "viagra" "nicht jugendfreie Websites" "Nicht jugendfreie Websites" "Jetzt zugreifen! Chance nicht verpassen!"
Wörterbuch für reguläre Ausdrücke mit Schlüsselwörtern im Zusammenhang mit Autorisierung	/(kennwort|kennwrt|kennw)[^a-z0-9]{1,3}(admin|anmelden|kennwort|benutzer)/i /(kunde|benutzer)[^a-z0-9]{1,3}konto[^a-z0-9]{1,3}nummer/i /fond[^a-z0-9]{1,3}transaktion/i /fond[^a-z0-9]{1,3}überweisung[^a-z0-9]{1,3}[0-9,.]+/i
Wörterbuch für Zeichenfolgen mit Hash-Werten für bekannte ungültige ausführbare Dateien	"fec72ceae15b6f60cbf269f99b9888e9" "fed472c13c1db095c4cb0fc54ed28485" "feddedb607468465f9428a59eb5ee22a" "ff3cb87742f9b56dfdb9a49b31c1743c" "ff45e471aa68c9e2b6d62a82bbb6a82a" "ff669082faf0b5b976cec8027833791c" "ff7025e261bd09250346bc9efdfc6c7c"
IP-Adressen wichtiger Ressourcen	192.168.1.12 192.168.2.0/24 192.168.3.0/255.255.255.0 192.168.4.32/27 192.168.5.144/255.255.255.240

Tabelle 3-26 Zweispaltiges Wörterbuch, Beispiele

Typ des Wörterbuchs	Beispiel
Wörterbuch für Zeichenfolgen mit allgemeinen Spam-Wörtern und -Kategorien	"Cialis" "pharmazeutisch" "cialis" "pharmazeutisch" "Viagra" "pharmazeutisch" "viagra" "pharmazeutisch" "nicht jugendfreie Website" "nicht jugendfrei" "Nicht jugendfreie Website" "nicht jugendfrei" "Jetzt zugreifen! Chance nicht verpassen!" "scam"
Wörterbuch für reguläre Ausdrücke mit Schlüsselwörtern und Kategorien im Zusammenhang mit Autorisierung	/(kennwort|kennwrt|kennw)[^a-z0-9]{1,3}(admin|anmelden|kennwort|benutzer)/i "anmeldeinformationen" /(kunde|benutzer)[^a-z0-9]{1,3}konto[^a-z0-9]{1,3}nummer/i "pii" /fond[^a-z0-9]{1,3}transaktion/i "sox" /fond[^a-z0-9]{1,3}überweisung[^a-z0-9]{1,3}[0-9,.]+/i "sox"
Wörterbuch für Zeichenfolgen mit Hash-Werten für bekannte ungültige ausführbare Dateien und Kategorien	"fec72ceae15b6f60cbf269f99b9888e9" "Trojaner" "fed472c13c1db095c4cb0fc54ed28485" "Malware" "feddedb607468465f9428a59eb5ee22a" "Virus" "ff3cb87742f9b56dfdb9a49b31c1743c" "Malware" "ff45e471aa68c9e2b6d62a82bbb6a82a" "Adware" "ff669082faf0b5b976cec8027833791c" "Trojaner" "ff7025e261bd09250346bc9efdfc6c7c" "Virus"
IP-Adressen wichtiger Ressourcen und Gruppen	192.168.1.12 "Wichtige Ressourcen" 192.168.2.0/24 "LAN" 192.168.3.0/255.255.255.0 "LAN" 192.168.4.32/27 "DMZ" 192.168.5.144/255.255.255.240 "Wichtige Ressourcen"

Verwalten von ADM-Wörterbüchern

Wenn Sie ein neues Wörterbuch eingerichtet und gespeichert haben, müssen Sie es in ESM importieren. Sie können das Wörterbuch auch exportieren, bearbeiten und löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im **Richtlinien-Editor** auf **Extras**, und wählen Sie dann **ADM-Wörterbuch-Manager** aus.

Auf dem Bildschirm **ADM-Wörterbücher verwalten** werden die vier Standardwörterbücher (botnet, foullanguage, icd9_desc und spamlist) sowie alle in das System importierten Wörterbücher aufgeführt.

2 Führen Sie eine oder mehrere der verfügbaren Aktionen aus, und klicken Sie dann auf **Schließen**.

Verweisen auf ein ADM-Wörterbuch

Wenn Sie ein Wörterbuch in ESM importieren, können Sie beim Schreiben von Regeln auf dieses Wörterbuch verweisen.

Bevor Sie beginnen
Importieren Sie das Wörterbuch in ESM.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im **Richtlinien-Editor** im Bereich **Regeltypen** auf **Neu** | **ADM-Regel**.

2 Fügen Sie die erforderlichen Informationen hinzu, ziehen Sie ein logisches Element in den Bereich **Ausdruckslogik**, und legen Sie es dort ab.

3 Ziehen Sie das Symbol **Ausdruckskomponente**  auf das logische Element, und legen Sie es dort ab.

4 Wählen Sie auf der Seite **Ausdruckskomponente** im Feld **Wörterbuch** das Wörterbuch aus.

5 Füllen Sie die verbleibenden Felder aus, und klicken Sie dann auf **OK**.

Referenzmaterial für ADM-Regeln

Dieser Anhang enthält Informationen, die Sie beim Hinzufügen von ADM-Regeln zum **Richtlinien-Editor** zu Hilfe nehmen können.

Syntax für ADM-Regeln

Die ADM-Regeln haben große Ähnlichkeit mit C-Ausdrücken.

Der Hauptunterschied besteht darin, dass es mehr Literale gibt (Zahlen, Zeichenfolgen, reguläre Ausdrücke, IP-Adressen, MAC-Adressen und boolesche Werte). Zeichenfolgenbegriffe können mit Zeichenfolgenliteralen und regulären Ausdrucksliteralen verglichen werden, um deren Inhalt zu testen. Sie können jedoch auch mit Zahlen verglichen werden, um deren Länge zu testen. Numerische Begriffe, IP-Adressbegriffe und MAC-Adressbegriffe können nur mit Literalwerten des gleichen Typs verglichen werden. Einzige Ausnahme: Alle Begriffe können als boolesche Werte behandelt werden, um zu testen, ob sie vorhanden sind. Manche Begriffe können mehrere Werte haben. So würde beispielsweise die folgende Regel für PDF-Dateien in ZIP-Dateien ausgelöst: type = = application/zip && type = = application/pdf.

Tabelle 3-27 Operatoren

Operator	Beschreibung	Beispiel
&&	Logisches AND	protocol = = http && type = = image/gif
||	Logisches OR	time.hour < 8 || time.hour > 18
^ ^	Logisches XOR	email.from = = "a@b.com" ^^email.to = = "a@b.com"
!	Unäres NOT	! (protocol = = http | | protocol = = ftp)
= =	Gleich	type = = application/pdf
! =	Nicht gleich	srcip ! = 192.168.0.0/16
>	Größer	objectsize > 100M
> =	Größer oder gleich	time.weekday > = 1

Tabelle 3-27 Operatoren *(Fortsetzung)*

Operator	Beschreibung	Beispiel
<	Kleiner	objectsize < 10K
< =	Kleiner oder gleich	time.hour < = 6

Tabelle 3-28 Literale

Literal	Beispiel
Zahl	1234, 0x1234, 0777, 16K, 10M, 2G
Zeichenfolge	"eine Zeichenfolge"
Regulärer Ausdruck	/[A-Z] [a-z]+/
IPv4	1.2.3.4, 192.168.0.0/16, 192.168.1.0/255.255.255.0
MAC	aa:bb:cc:dd:ee:ff
Boolescher Wert	wahr, falsch

Tabelle 3-29 Kompatibilität der Typen und Operatoren

Typ	Operatoren	Hinweise
Zahl	= =, ! =, >, > =, <, < =	
Zeichenfolge	= =, ! =	Zum Vergleichen des Inhalts einer Zeichenfolge mit Zeichenfolge/regulärer Ausdruck
Zeichenfolge	>, > =, <, <=	Zum Vergleichen der Länge einer Zeichenfolge
IPv4	= =, ! =	
MAC	= =, ! =	
Boolescher Wert	= =, ! =	Zum Vergleichen mit wahr/falsch, unterstützt außerdem den impliziten Vergleich mit wahr, beispielsweise in den folgenden Tests, ob der Begriff email.bcc auftritt: email.bcc

Tabelle 3-30 ADM, reguläre Ausdrücke, Grammatik

Einfache Operatoren	
|	Alternierung (oder)
*	Null oder mehr
+	Eins oder mehr
?	Null oder mehr
( )	Gruppierung (a | b)
{ }	Wiederholter Bereich {x} oder {,x} oder {x,} oder {x,y}
[ ]	Bereich [0-9a-z] [abc]
[^]	Ausschließlicher Bereich [^abc] [^0-9]
.	Beliebiges Zeichen
\	Escape-Zeichen

Escape-Zeichen	
\d	Ziffer [0-9]
\D	Nicht-Ziffer [^0-9]
\e	Escape-Zeichen (0x1B)
\f	Seitenvorschub (0x0C)
\n	Zeilenvorschub (0x0A)
\r	Wagenrücklauf (0x0D)
\s	Leerzeichen
\S	Nicht Leerzeichen
\t	Tabstopp (0x09)
\v	Vertikaler Tabstopp (0x0B)
\w	Wort [A-Za-z0-9_]
\W	Nicht Wort
\x00	Darstellung im Hexadezimalformat
\0000	Darstellung im Oktalformat
^	Zeilenanfang
S	Zeilenende
	Die Anker für Zeilenanfang und Zeilenende (^ und $) funktionieren für objcontent nicht.

POSIX-Zeichenklassen	
[:alunum:]	Ziffern und Buchstaben
[:alpha:]	Alle Buchstaben
[:ascii:]	ASCII-Zeichen
[:blank:]	Leerzeichen und Tabstopp
[:cntrl:]	Steuerzeichen
[:digit:]	Ziffern
[:graph:]	Sichtbare Zeichen
[:lower:]	Kleinbuchstaben
[:print:]	Sichtbare Zeichen und Leerzeichen
[:punct:]	Satzzeichen und Symbole
[:space:]	Alle Leerraumzeichen
[:upper:]	Großbuchstaben

POSIX-Zeichenklassen	
[:word:]	Wortzeichen
[:xdigit:]	Ziffer im Hexadezimalformat

Begriffstypen für ADM-Regeln

Alle Begriffe in einer ADM-Regel haben einen bestimmten Typ.

Jeder Begriff ist entweder eine IP-Adresse, eine MAC-Adresse, eine Zahl, eine Zeichenfolge oder ein boolescher Wert. Außerdem gibt es zwei zusätzliche Literaltypen: reguläre Ausdrücke und Listen. Ein Begriff eines bestimmten Typs kann im Allgemeinen nur mit einem Literal des gleichen Typs oder mit einer Liste von Literalen des gleichen Typs (oder einer Liste von Listen von Literalen) verglichen werden. Für diese Regel gelten drei Ausnahmen:

1. Ein Zeichenfolgenbegriff kann mit einem numerischen Literal verglichen werden, um seine Länge zu testen. Die folgende Regel wird ausgelöst, wenn ein Kennwort aus weniger als acht Zeichen besteht (password ist ein Zeichenfolgenbegriff): password < 8
2. Ein Zeichenfolgenbegriff kann mit einem regulären Ausdruck verglichen werden. Die folgende Regel wird ausgelöst, wenn ein Kennwort nur Kleinbuchstaben enthält: password == /^[a-z]+$/
3. Alle Begriffe können anhand von booleschen Literalwerten darauf getestet werden, ob sie überhaupt vorkommen. Die folgende Regel wird ausgelöst, wenn eine E-Mail eine Cc-Adresse enthält (email.cc ist ein Zeichenfolgenbegriff): email.cc == true

Typ	Formatbeschreibung
IP-Adressen	• IP-Adressliterale werden in standardmäßiger Dotted Quad-Notation geschrieben und nicht in Anführungszeichen eingeschlossen: 192.168.1.1 • Für IP-Adressen kann eine Maske in der standardmäßigen CIDR-Schreibweise geschrieben werden, die keine Leerzeichen zwischen Adresse und Maske enthalten darf: 192.168.1.0/24 • Für IP-Adressen können auch Masken in langer Form geschrieben werden: 192.168.1.0/255.255.255.0
MAC-Adressen	• MAC-Adressliterale werden in der Standardschreibweise geschrieben und wie IP-Adressen nicht in Anführungszeichen eingeschlossen: aa:bb:cc:dd:ee:ff
Zahlen	• Alle Zahlen in ADM-Regeln sind 32-Bit-Ganzzahlen. Sie können im Dezimalformat geschrieben werden: 1234 • Sie können im Hexadezimalformat geschrieben werden: 0xabcd • Sie können im Oktalformat geschrieben werden: 0777 • Sie können über einen angefügten Multiplikator verfügen: Multiplikation mit 1024 (K), 1048576 (M) oder 1073741824 (G): 10M

Typ	Formatbeschreibung
Zeichenfolgen	• Zeichenfolgen werden in doppelte Anführungszeichen eingeschlossen: "dies ist eine Zeichenfolge" • In Zeichenfolgen können standardmäßige C-Escape-Sequenzen verwendet werden: "\tDies ist eine \"Zeichenfolge\" mit\x20Escape-Sequenzen\n" • Beim Vergleichen eines Begriffs mit einer Zeichenfolge muss der gesamte Begriff mit der Zeichenfolge übereinstimmen. Wenn eine E-Mail-Nachricht die Absenderadresse jemand@irgendwo.com enthält, wird die folgende Regel nicht ausgelöst: email.from == "@irgendwo.com" • Wenn Sie nur einen Teil eines Begriffs vergleichen möchten, müssen Sie stattdessen ein reguläres Ausdrucksliteral verwenden. Verwenden Sie nach Möglichkeit Zeichenfolgenliterale, da diese effizienter sind.  Alle Begriffe für E-Mail-Adressen und URLs werden vor dem Vergleich normalisiert. Daher müssen beispielsweise Kommentare in E-Mail-Adressen nicht berücksichtigt werden.
Boolesche Werte	• Die booleschen Literalwerte lauten wahr und falsch.

Typ	Formatbeschreibung
Reguläre Ausdrücke	• Für reguläre Ausdrucksliterale wird die gleiche Schreibweise wie in Sprachen wie JavaScript und Perl verwendet. Dabei wird der reguläre Ausdruck in Schrägstriche eingeschlossen: /[a-z]+/ • Reguläre Ausdrücke können von einer Kennzeichnung durch einen Standardmodifizierer gefolgt sein. Zurzeit wird jedoch nur "i" (Groß-/Kleinschreibung ignorieren) erkannt: /[a-z]+/i • Für reguläre Ausdrucksliterale sollten Sie die erweiterte POSIX-Syntax verwenden. Zurzeit funktionieren zwar Perl-Erweiterungen für alle Begriffe mit Ausnahme des Inhaltsbegriffs, dies kann sich jedoch in zukünftigen Versionen ändern. • Beim Vergleich eines Begriffs mit einem regulären Ausdruck werden alle Teilzeichenfolgen im Begriff verglichen, sofern nicht innerhalb des regulären Ausdrucks Anker-Operatoren angewendet werden. Die folgende Regel wird ausgelöst, wenn eine E-Mail mit der Adresse "jemand@irgendwo.com" gefunden wird: email.from == /@irgendwo.com/
Listen	• Listenliterale bestehen aus mindestens einem in eckige Klammern eingeschlossenen Literal und werden durch Kommas getrennt: [1, 2, 3, 4, 5] • Listen könnten alle Arten von Literalen enthalten, auch andere Listen: [192.168.1.1, [10.0.0.0/8, 172.16.128.0/24]] • Listen dürfen nur eine Art von Literal enthalten. Kombinationen aus Zeichenfolgen und Zahlen, Zeichenfolgen und regulären Ausdrücken oder IP-Adressen und MAC-Adressen sind nicht gültig. • Wenn eine Liste mit einem relationalen Operator außer dem Operator für nicht gleich (!=) verwendet wird, ist der Ausdruck wahr, wenn der Begriff mit einem beliebigen Literal in der Liste übereinstimmt. Die folgende Regel wird ausgelöst, wenn die Quell-IP-Adresse mit einer der IP-Adressen in der Liste übereinstimmt: srcip == [192.168.1.1, 192.168.1.2, 192.168.1.3] • Dies entspricht: srcip == 192.168.1.1 || srcip == 192.168.1.2 || srcip == 192.168.1.3 • Bei Verwendung mit dem Operator für nicht gleich (!=) ist der Ausdruck wahr, wenn der Begriff nicht mit allen Literalen in der Liste übereinstimmt. Die folgende Regel wird ausgelöst, wenn die Quell-IP-Adresse nicht 192.168.1.1 oder 192.168.1.2 entspricht: srcip != [192.168.1.1, 192.168.1.2] • Dies entspricht: srcip != 192.168.1.1 && srcip != 192.168.1.2 • Listen können auch mit den anderen relationalen Operatoren verwendet werden, obwohl dies nicht sehr sinnvoll ist. Die folgende Regel wird ausgelöst, wenn die Objektgröße größer als 100 oder 200 ist: objectsize > [100, 200] • Dies entspricht: objectsize > 100 || objectsize > 200

Messgrößenreferenzen für ADM-Regeln

Nachfolgend finden Sie Listen mit Messgrößenreferenzen für die ADM-Regelausdrücke, die beim Hinzufügen einer ADM-Regel auf der Seite **Ausdruckskomponente** zur Verfügung stehen.

Für allgemeine Eigenschaften und allgemeine Anomalien werden die Parametertypwerte, die Sie jeweils eingeben können, in Klammern hinter der Messgrößenreferenz gezeigt.

Allgemeine Eigenschaften

Eigenschaft oder Begriff	Beschreibung
Protokoll (Zahl)	Anwendungsprotokoll (HTTP, FTP, SMTP)
Objektinhalt (Zeichenfolge)	Der Inhalt eines Objekts (Text in einem Dokument, einer E-Mail-Nachricht oder einer Chat-Nachricht). Kontextübereinstimmung ist für Binärdaten nicht verfügbar. Binärobjekte können jedoch mithilfe des Objekttyps (objtype) entdeckt werden.
Objekttyp (Zahl)	Gibt den von ADM ermittelten Typ des Inhalts an (Office-Dokumente, Nachrichten, Videos, Audio, Bilder, Archive, ausführbare Dateien).
Objektgröße (Zahl)	Größe des Objekts. Nach der Zahl können die numerischen Multiplikatoren K, M und G hinzugefügt werden (10K, 10M, 10G).
Objekt-Hash (Zeichenfolge)	Der Hash des Inhalts (zurzeit MD5)
Quell-IP-Adresse des Objekts (Zahl)	Die Quell-IP-Adresse des Inhalts. Die IP-Adresse kann als 192.168.1.1, 192.168.1.0/24 oder 192.168.1.0/255.255.255.0 angegeben werden.
Ziel-IP-Adresse des Objekts (Zahl)	Die Ziel-IP-Adresse des Inhalts. Die IP-Adresse kann als 192.168.1.1, 192.168.1.0/24 oder 192.168.1.0/255.255.255.0 angegeben werden.
Quell-Port des Objekts (Zahl)	Der TCP/UDP-Quell-Port des Inhalts
Ziel-Port des Objekts (Zahl)	Der TCP/UDP-Ziel-Port des Inhalts
Quell-IPv6-Adresse des Objekts (Zahl)	Die Quell-IPv6-Adresse des Inhalts
Ziel-IPv6-Adresse des Objekts (Zahl)	Die Ziel-IPv6-Adresse des Inhalts
MAC-Quelladresse des Objekts (MAC-Name)	Die MAC-Quelladresse des Inhalts (aa:bb:cc:dd:ee:ff)
MAC-Zieladresse des Objekts (MAC-Name)	Die MAC-Zieladresse des Inhalts (aa:bb:cc:dd:ee:ff)
Quell-IP-Adresse des Flusses (IPv4)	Quell-IP-Adresse des Flusses. Die IP-Adresse kann als 192.168.1.1, 192.168.1.0/24 oder 192.168.1.0/255.255.255.0 angegeben werden.
Ziel-IP-Adresse des Flusses (IPv4)	Ziel-IP-Adresse des Flusses. Die IP-Adresse kann als 192.168.1.1, 192.168.1.0/24 oder 192.168.1.0/255.255.255.0 angegeben werden.
Quell-Port des Flusses (Zahl)	TCP/UDP-Quell-Port des Flusses
Ziel-Port des Flusses (Zahl)	TCP/UDP-Ziel-Port des Flusses
Quell-IPv6-Adresse des Flusses (Zahl)	Quell-IPv6-Adresse des Flusses
Ziel-IPv6-Adresse des Flusses (Zahl)	Ziel-IPv6-Adresse des Flusses
MAC-Quelladresse des Flusses (MAC-Name)	MAC-Quelladresse des Flusses
MAC-Zieladresse des Flusses (MAC-Name)	MAC-Zieladresse des Flusses
VLAN (Zahl)	Virtuelle LAN-ID
Wochentag (Zahl)	Der Tag der Woche. Gültige Werte: 1 bis 7, 1 steht für Montag.
Stunde (Zahl)	Die Tageszeit gemäß GMT. Gültige Werte: 0 bis 23.

Eigenschaft oder Begriff	Beschreibung
Deklarierter Inhaltstyp (Zeichenfolge)	Der vom Server angegebene Typ des Inhalts. Theoretisch entspricht der Objekttyp (objtype) immer dem tatsächlichen Typ, und der deklarierte Inhaltstyp (content-type) ist nicht vertrauenswürdig, da er vom Server oder der Anwendung gefälscht werden kann.
Kennwort (Zeichenfolge)	Das von der Anwendung für die Authentifizierung verwendete Kennwort
URL (Zeichenfolge)	Website-URL. Gilt nur für das HTTP-Protokoll.
Dateiname (Zeichenfolge)	Der Name der übertragenen Datei
Anzeigename (Zeichenfolge)	
Hostname (Zeichenfolge)	Der bei der DNS-Suche angegebene Hostname

Allgemeine Anomalien

- Abmeldung des Benutzers (boolescher Wert)
- Autorisierungsfehler (boolescher Wert)
- Autorisierung erfolgreich (boolescher Wert)
- Autorisierung fehlgeschlagen (boolescher Wert)

Protokollspezifische Eigenschaften

Neben den Eigenschaften, die den meisten Protokollen gemeinsam sind, enthält ADM protokollspezifische Eigenschaften, die für ADM-Regeln verwendet werden können. Alle protokollspezifischen Eigenschaften stehen auch beim Hinzufügen einer ADM-Regel auf der Seite **Ausdruckskomponente** zur Verfügung.

Beispiele für protokollspezifische Eigenschaften

Diese Eigenschaften gelten für die folgenden Tabellen:

```
* Nur Entdeckung
** Keine Entschlüsselung, zeichnet X.509-Zertifikate und verschlüsselte Daten auf
*** Über RFC822-Modul
```

Tabelle 3-31 Module von Dateiübertragungsprotokollen

FTP	HTTP	SMB*	SSL**
Anzeigename	Anzeigename	Anzeigename	Anzeigename
Dateiname	Dateiname	Dateiname	Dateiname
Hostname	Hostname	Hostname	Hostname
URL	Referenz		
	URL		
	Alle HTTP-Header		

Tabelle 3-32 Module von E-Mail-Protokollen

DeltaSync	MAPI	NNTP	POP3	SMTP
Bcc***	Bcc	Bcc***	Bcc***	Bcc***
Cc***	Cc	Cc***	Cc***	Cc***
Anzeigename	Anzeigename	Anzeigename	Anzeigename	Anzeigename
Von***	Von	Von***	Von***	Von***
Hostname	Hostname	Hostname	Hostname	Hostname
Betreff***	Betreff	Betreff***	Betreff***	An***
An***	An	An***	An***	Betreff***
	Benutzername		Benutzername	

Tabelle 3-33 Module von Web-Mail-Protokollen

AOL	Gmail	Hotmail	Yahoo
Anhangsname	Anhangsname	Anhangsname	Anhangsname
Bcc***	Bcc***	Bcc***	Bcc***
Cc***	Cc***	Cc***	Cc***
Anzeigename	Anzeigename	Anzeigename	Anzeigename
Dateiname	Dateiname	Dateiname	Dateiname
Hostname	Hostname	Hostname	Hostname
Von***	Von***	Von***	Von***
Betreff***	Betreff***	Betreff***	Betreff***
An***	An***	An***	An***

Protokollanomalien

Neben den allgemeinen und protokollspezifischen Eigenschaften können mit ADM auch Hunderte von Anomalien in Low-Level-Protokollen, Transport- und Anwendungsprotokollen entdeckt werden. Alle Eigenschaften von Protokollanomalien entsprechen dem Typ Boolescher Wert und stehen beim Hinzufügen einer ADM-Regel auf der Seite **Ausdruckskomponente** zur Verfügung.

Tabelle 3-34 IP

Begriff	Beschreibung
ip.too-small	Das IP-Paket ist zu klein, um einen gültigen Header zu enthalten.
ip.bad-offset	Der IP-Daten-Offset geht über das Ende des Pakets hinaus.
ip.fragmented	Das IP-Paket ist fragmentiert.
ip.bad-checksum	Die Prüfsumme des IP-Pakets stimmt nicht mit den Daten überein.
ip.bad-length	Das totlen-Feld des IP-Pakets geht über das Ende des Pakets hinaus.

Tabelle 3-35 TCP

Begriff	Beschreibung
tcp.too-small	Das TCP-Paket ist zu klein, um einen gültigen Header zu enthalten.
tcp.bad-offset	Der Daten-Offset des TCP-Pakets geht über das Ende des Pakets hinaus.

Tabelle 3-35 TCP *(Fortsetzung)*

Begriff	Beschreibung
tcp.unexpected-fin	Die TCP-Markierung FIN ist festgelegt, obwohl die Verbindung nicht hergestellt wurde.
tcp.unexpected-syn	Die TCP-Markierung SYN ist festgelegt, obwohl die Verbindung hergestellt wurde.
tcp.duplicate-ack	Für das TCP-Paket wird eine ACK-Nachricht für Daten gesendet, für die bereits eine ACK-Nachricht gesendet wurde.
tcp.segment-outsidewindow	Das TCP-Paket befindet sich außerhalb des Fensters (das kleine Fenster des TCP-Moduls, nicht das tatsächliche Fenster).
tcp.urgent-nonzero-withouturg- flag	Das TCP-Feld urgent entspricht nicht null, aber die URG-Markierung ist nicht festgelegt.

Tabelle 3-36 DNS

Begriff	Beschreibung
dns.too-small	Das DNS-Paket ist zu klein, um einen gültigen Header zu enthalten.
dns.question-name-past-end	Der Name der DNS-Frage geht über das Ende des Pakets hinaus.
dns.answer-name-past-end	Der Name der DNS-Antwort geht über das Ende des Pakets hinaus.
dns.ipv4-address-length-wrong	Die IPv4-Adresse in der DNS-Antwort ist nicht vier Byte lang.
dns.answer-circular-reference	Die DNS-Antwort enthält einen Zirkelverweis.

Einstellungen für Database Event Monitor (DEM)

Mit McAfee Database Event Monitor (DEM) werden Datenbankaktivitäten in einem zentralen Audit-Repository konsolidiert und die einzelnen Aktivitäten werden normalisiert, korreliert, analysiert und in Berichten erfasst. Wenn Aktivitäten im Netzwerk oder auf einem Datenbank-Server mit bekannten Mustern übereinstimmen, die auf bösartigen Datenzugriff hinweisen, wird durch DEM eine Warnung generiert. Außerdem werden alle Transaktionen zu Compliance-Zwecken protokolliert.

Sie können mit DEM Datenbank-Überwachungsregeln über die gleiche Benutzeroberfläche verwalten, bearbeiten und anpassen, die Sie zu Analyse- und Berichterstellungszwecken verwenden. Auf diese Weise können Sie leicht bestimmte Datenbank-Überwachungsprofile anpassen (welche Regeln erzwungen werden, welche Transaktionen protokolliert werden) und so die Anzahl der False-Positives reduzieren und die allgemeine Sicherheit verbessern.

Die Interaktionen der Benutzer und Anwendungen mit den Datenbanken werden ohne Störungen in DEM überwacht. Dazu werden Netzwerkpakete ähnlich wie bei Systemen zur Erkennung von Eindringungsversuchen überwacht. Stellen Sie sicher, dass Sie alle Aktivitäten auf Datenbank-Servern über das Netzwerk überwachen können, indem Sie die anfängliche DEM-Bereitstellung mit den Teams aus den Bereichen Netzwerk, Sicherheit, Compliance und Datenbanken koordinieren.

Die Netzwerkteams können Span-Ports an Switches, Netzwerk-Taps oder Hubs verwenden, um den Datenbankverkehr zu replizieren. So können Sie den Datenverkehr auf den Datenbank-Servern abhören oder überwachen und ein Audit-Protokoll erstellen.

Informationen zu den unterstützten Datenbank-Server-Plattformen und Versionen finden Sie auf der McAfee-Website.

Betriebssystem	Database	DEM-Appliance	DEM-Agent
Windows (alle Versionen)	Microsoft SQL Server[1]	MSSQL 7, 2000, 2005, 2008, 2012	MSSQL 2000 (SP4), 2005, 2008
Windows, UNIX/Linux (alle Versionen)	Oracle[2]	Oracle 8.X, 9.X, 10 g, 11 g (c), 11 g R2[3]	Oracle 8.0.3+, 9.X, 10.X, 11.X
	Sybase	11.X, 12.X, 15.X	11.X, 12.X, 15.X
	DB2	8.X, 9.X, 10.X	7,1.X, 8.X, 9.X
	Informix (verfügbar in 8.4.0 und höher)	11.5	--
Windows, UNIX/Linux (alle Versionen)	MySQL	Ja, 4.X, 5.X, 6.X	Ja, 4.1.22.X, 5.0.3X
	PostgreSQL	7.4.X, 8.4.X, 9.0.X, 9.1.X	--
	Teradata	12.x, 13.x, 14.x	--
	InterSystems Caché	2011,1.x	--
UNIX/Linux (alle Versionen)	Greenplum	8.2.15	--
	Vertica	5.1.1-0	--
Mainframe	DB2/zOS	Alle Versionen	Option für Partner-Agenten
AS400	DB2	Alle Versionen	--

1 Die Paketentschlüsselung für Microsoft SQL Server wird in Version 8.3.0 und höher unterstützt.

2 Die Paketentschlüsselung für Oracle wird in Version 8.4.0 und höher unterstützt.

3 Oracle 11g ist in Version 8.3.0 und höher verfügbar.

Für die genannten Server und Versionen gilt Folgendes:

- Es werden die 32-Bit- und 64-Bit-Versionen von Betriebssystemen und Datenbankplattformen unterstützt.
- MySQL wird nur auf Windows-32-Bit-Plattformen unterstützt.
- Die Paketentschlüsselung wird für MSSQL und Oracle unterstützt.

DEM-Lizenz aktualisieren

Im Lieferumfang des DEM-Geräts ist eine Standardlizenz enthalten. Wenn Sie die Funktionen des DEM-Geräts ändern, erhalten Sie von McAfee per E-Mail eine neue Lizenz und müssen die Lizenz aktualisieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **DEM-Konfiguration**.

2 Klicken Sie auf **Lizenz** | **Lizenz aktualisieren**, und fügen Sie dann die von McAfee erhaltenen Informationen in das Feld ein.

3 Klicken Sie auf **OK**.

Die Lizenz wird im System aktualisiert, und Sie werden anschließend informiert.

4 Führen Sie einen Rollout für die Richtlinie auf dem DEM-Gerät aus.

Synchronisieren von DEM-Konfigurationsdateien

Wenn die DEM-Konfigurationsdateien nicht mit dem DEM-Gerät synchronisiert sind, müssen Sie die Konfigurationsdateien in das DEM-Gerät schreiben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **DEM-Konfiguration**.

2 Klicken Sie auf **Dateien synchronisieren**.

Der Status der Synchronisierung wird in einer Meldung angezeigt.

Erweiterte DEM-Einstellungen konfigurieren

Mit diesen erweiterten Einstellungen können Sie die Leistung des DEM-Geräts ändern oder erhöhen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **DEM-Konfiguration**.

2 Klicken Sie auf **Erweitert**, und definieren Sie dann die Einstellungen, oder heben Sie die Auswahl von Optionen auf, wenn das DEM-Gerät stark ausgelastet ist.

3 Klicken Sie auf **OK**.

Anwenden von DEM-Konfigurationseinstellungen

Änderungen an DEM-Konfigurationseinstellungen müssen auf das DEM-Gerät angewendet werden. Wenn Sie nicht alle Konfigurationseinstellungen angewendet haben, können Sie dies mit der Option **Anwenden** in **DEM-Konfiguration** für alle DEM-Konfigurationseinstellungen nachholen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **DEM-Konfiguration**.

2 Klicken Sie auf **Anwenden**.

Beim Schreiben der Konfigurationseinstellungen in das DEM-Gerät wird eine Meldung angezeigt.

Definieren von Aktionen für DEM-Ereignisse

Mit den Einstellungen für **Aktionsverwaltung** im DEM-Gerät definieren Sie Aktionen und Vorgänge für Ereignisse, die in den Filterregeln und Datenzugriffsrichtlinien des DEM-Geräts verwendet werden. Sie

können benutzerdefinierte Aktionen hinzufügen und den **Vorgang** für Standardaktionen und benutzerdefinierte Aktionen festlegen.

Im Lieferumfang des DEM-Geräts sind Standardaktionen enthalten, die Sie anzeigen können, indem Sie auf der Seite **Aktionsverwaltung** auf **Global bearbeiten** klicken. Außerdem sind die folgenden Standardvorgänge enthalten:

- **Keine**
- **Ignorieren**
- **Verwerfen**
- **Skript**
- **Zurücksetzen**

Wenn Sie den Vorgang **Skript** auswählen, ist ein Alias-Name erforderlich (SKRIPT-ALIAS), der auf das eigentliche Skript (SKRIPTNAME) verweist, das beim Auftreten des Ereignisses mit der entsprechenden Wichtigkeit ausgeführt werden muss. Dem Skript werden zwei Umgebungsvariablen übergeben, ALERT_EVENT und ALERT_REASON. ALERT_EVENT enthält eine durch Doppelpunkte getrennte Liste mit Messgrößen. DEM enthält ein Beispiel für ein Bash-Skript (/home/auditprobe/conf/sample/process_alerts.bash), mit dem veranschaulicht wird, wie die Aktion für die Wichtigkeit in einem Skript aufgezeichnet werden kann.

Beachten Sie beim Arbeiten mit Aktionen und Vorgängen Folgendes:

- Aktionen werden nach Priorität aufgeführt.
- Bei Ereignissen werden Aktionen wie beispielsweise das Senden eines SNMP-Traps oder einer Seite nur ausgeführt, wenn Sie dies als Warnungsaktion festlegen.
- Wenn eine Regel für mehrere Warnungsstufen gilt, können nur für die höchste Warnungsstufe Aktionen ausgeführt werden.
- Ereignisse werden unabhängig von der Aktion in eine Ereignisdatei geschrieben. Die einzige Ausnahme davon ist der Vorgang **Verwerfen**.

Hinzufügen einer DEM-Aktion

Wenn Sie in der DEM-Aktionsverwaltung eine Aktion hinzufügen, wird diese in der Liste der verfügbaren Aktionen für eine DEM-Regel im **Richtlinien-Editor** angezeigt. Sie können die Aktion dann als Aktion für eine Regel auswählen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der Systemnavigationsstruktur auf das Symbol **Richtlinien-Editor** und dann auf **Extras | DEM-Aktions-Manager**.

Auf der Seite **DEM-Aktionsverwaltung** werden die vorhandenen Aktionen in der Reihenfolge ihrer Priorität aufgeführt.

Die Priorität der Standardaktionen können Sie nicht ändern.

2 Klicken Sie auf **Hinzufügen**, und geben Sie dann einen Namen und eine Beschreibung für die Aktion ein.

Eine hinzugefügte benutzerdefinierte Aktion können Sie nicht löschen.

3 Klicken Sie auf **OK**.

Die neue Aktion wird zur Liste **DEM-Aktionsverwaltung** hinzugefügt.

Der Standardvorgang für eine benutzerdefinierte Aktion lautet **Keine**. Informationen zum Ändern des Standardvorgangs finden Sie unter *Festlegen des Vorgangs für eine DEM-Aktion*.

Bearbeiten einer benutzerdefinierten DEM-Aktion

Möglicherweise müssen Sie den Namen einer zur Liste DEM-Aktionsverwaltung hinzugefügten Aktion bearbeiten oder die Priorität der Aktion ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Systemnavigationsstruktur auf das Symbol **Richtlinien-Editor** und dann auf **Extras** | **DEM-Aktions-Manager**.
2. Klicken Sie auf die benutzerdefinierte Aktion, die Sie ändern möchten, und führen Sie einen der folgenden Schritte aus:
   - Zum Ändern der Priorität klicken Sie auf den Pfeil nach oben oder nach unten, bis sich die Aktion an der richtigen Position befindet.
   - Zum Ändern des Namens oder der Beschreibung klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Festlegen des Vorgangs für eine DEM-Aktion

Für alle Regelaktionen gibt es einen Standardvorgang. Wenn Sie eine benutzerdefinierte DEM-Aktion hinzufügen, lautet der Standardvorgang **Keine**. Sie können den Vorgang für eine Aktion in **Ignorieren**, **Verwerfen**, **Skript** oder **Zurücksetzen** ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **Aktionsverwaltung**.
2. Heben Sie die zu bearbeitende Aktion hervor, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie einen Vorgang aus, und klicken Sie dann auf **OK**.

Arbeiten mit Masken für vertrauliche Daten

Mit Masken für vertrauliche Daten verhindern Sie das nicht autorisierte Anzeigen von vertraulichen Daten. Dabei werden die vertraulichen Informationen durch eine generische Zeichenfolge, die sogenannte Maske, ersetzt. Wenn Sie ein DEM-Gerät zum System hinzufügen, werden drei

Standardmasken für vertrauliche Daten zur ESM-Datenbank hinzugefügt. Sie können jedoch neue Masken hinzufügen und vorhandene Masken bearbeiten oder entfernen.

Die folgenden Standardmasken stehen zur Verfügung:

- Name der Maske für vertrauliche Daten: Maske für Kreditkartennummern

  Ausdruck: ((4\d{3})|(5[1-5]\d{2})|(6011))-?\d{4}-?\d{4}-?\d{4}|3[4,7]\d{13}

  Index der Teilzeichenfolgen: \0

  Maskierungsmuster: ####-####-####-####

- Name der Maske für vertrauliche Daten: Erste fünf Zeichen der SSN maskieren

  Ausdruck: (\d\d\d-\d\d)-\d\d\d\d

  Index der Teilzeichenfolgen: \1

  Maskierungsmuster: ###-##

- Name der Maske für vertrauliche Daten: Benutzerkennwort in SQL-Anweisung maskieren

  Ausdruck: create\s+user\s+(\w+)\s+identified\s+by\s+(\w+)

  Index der Teilzeichenfolgen: \2

  Maskierungsmuster: ********

Verwalten von Masken für vertrauliche Daten

Sie können im System eingegebene vertrauliche Informationen schützen, indem Sie Masken für vertrauliche Daten hinzufügen und vorhandene Masken bearbeiten oder entfernen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **Masken für vertrauliche Daten**.

2 Wählen Sie eine Option aus, und geben Sie dann die erforderlichen Informationen ein.

3 Klicken Sie auf **OK** und dann auf **Schreiben**, um die Einstellungen zum DEM-Gerät hinzuzufügen.

Verwalten der Benutzeridentifizierung

Ein großer Teil der Sicherheit basiert auf einem einfachen Prinzip: Benutzer müssen identifiziert und voneinander unterschieden werden. Dennoch werden für den Zugriff auf die Datenbank häufig generische Benutzernamen verwendet. Mithilfe der ID-Verwaltung können Sie den tatsächlichen

Benutzernamen aufzeichnen, wenn dieser an irgendeiner Stelle in der Abfrage enthalten ist. Dazu verwenden Sie Muster für reguläre Ausdrücke.

Anwendungen können relativ leicht so instrumentiert werden, dass diese Sicherheitsfunktion genutzt werden kann. Wenn Sie ein DEM-Gerät zum System hinzufügen, werden zwei definierte ID-Regeln zur ESM-Datenbank hinzugefügt.

- Name der ID-Regel: Benutzernamen aus SQL-Anweisung abrufen

  Ausdruck: select\s+username=(\w+)

  Anwendung: Oracle

  Index der Teilzeichenfolgen: \1

- Name der ID-Regel: Benutzernamen aus gespeicherter Prozedur abrufen

  Ausdruck: sessionStart\s+@appname='(\w+)', @username='(\w+)',

  Anwendung: MSSQL

  Index der Teilzeichenfolgen: \2

Eine erweiterte Korrelation der Benutzer ist möglich, indem Sie die Protokolle für DEM, Anwendung, Web-Server, System sowie für die Identitäts- und Zugriffsverwaltung in ESM korrelieren.

Hinzufügen einer Regel für Benutzer-IDs

Zum Zuordnen von Datenbankabfragen zu Personen können Sie die vorhandenen ID-Regeln verwenden oder eine neue Regel hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **ID-Verwaltung**.
2. Klicken Sie auf **Hinzufügen**, und geben Sie dann die erforderlichen Informationen ein.
3. Klicken Sie auf **OK** und dann auf **Schreiben**, um die Einstellungen in das DEM-Gerät zu schreiben.

Informationen zu Datenbank-Servern

Die Datenbankaktivitäten werden von den Datenbank-Servern überwacht. Wenn auf einem Datenbank-Server auftretende Aktivitäten einem bekannten Muster entsprechen, das auf böswilligen Datenzugriff hinweist, wird eine Warnung generiert. Mit jedem DEM-Gerät können maximal 255 Datenbank-Server überwacht werden.

Von DEM werden zurzeit die folgenden Datenbank-Server und Versionen unterstützt:

OS	Database	DEM-Appliance	DEM-Agent
Windows (alle Versionen)	Microsoft SQL Server[1]	MSSQL 7, 2000, 2005, 2008, 2012	MSSQL 2000 (SP4), 2005, 2008
Windows, UNIX/ Linux (alle Versionen)	Oracle[2]	Oracle 8.X, 9.X, 10g, 11g[3], 11g R2	Oracle 8.0.3+, 9.X, 10.X, 11.X
	Sybase	11.X, 12.X, 15.X	11.X, 12.X, 15.X
	DB2	8.X, 9.X, 10.X	7,1.X, 8.X, 9.X

OS	Database	DEM-Appliance	DEM-Agent
	Informix (siehe Hinweis 4)	11.5	--
	MySQL	Ja, 4.X, 5.X, 6.X	Ja, 4.1.22.X, 5.0.3X
	PostgreSQL	7.4.X, 8.4.X, 9.0.X, 9.1.X	--
	Teradata	12.x, 13.x, 14.x	--
	InterSystems Caché	2011,1.x	--
UNIX/Linux (alle Versionen)	Greenplum	8.2.15	--
	Vertica	5.1.1-0	--
Mainframe	DB2/zOS	Alle Versionen	Option für Partner-Agenten
AS/400	DB2	Alle Versionen	--

1 Die Paketentschlüsselung für Microsoft SQL Server wird in Version 8.3.0 und höher unterstützt.

2 Die Paketentschlüsselung für Oracle wird in Version 8.4.0 und höher unterstützt.

3 Oracle 11g ist in Version 8.3.0 und höher verfügbar.

4 Unterstützung für Informix ist in Version 8.4.0 und höher verfügbar.

- Es werden die 32-Bit- und 64-Bit-Versionen von Betriebssystemen und Datenbankplattformen unterstützt.
- DEM-Agenten werden in allen Betriebssystemversionen von Windows, UNIX und Linux unterstützt.
- Für DEM-Agenten ist Java Virtual Machine (JVM) erforderlich.
- MySQL wird nur auf Windows-32-Bit-Plattformen unterstützt.
- Die Paketentschlüsselung wird für MSSQL und Oracle unterstützt.

Verwalten von Datenbank-Servern

Die Seite **Datenbank-Server** stellt den Ausgangspunkt für die Verwaltung der Einstellungen für alle Datenbank-Server für das DEM-Gerät dar.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **Datenbank-Server**.
2. Wählen Sie eine der verfügbaren Optionen aus.
3. Klicken Sie auf **OK**.

Verwalten von Benachrichtigungen für die Datenbankerkennung

DEM verfügt über eine Funktion für die Datenbankerkennung, mit der Sie eine Ausnahmeliste der nicht überwachten Datenbank-Server erhalten. Auf diese Weise kann ein Sicherheitsadministrator zur Umgebung hinzugefügte neue Datenbank-Server erkennen sowie verbotene Listener-Ports, die geöffnet wurden, um auf Daten aus Datenbanken zuzugreifen. Wenn diese Funktion aktiviert ist, erhalten Sie eine Warnbenachrichtigung, die in der Ansicht **Ereignisanalyse** angezeigt wird. Dann können Sie auswählen, ob der Server zu den im System überwachten Servern hinzugefügt werden soll.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **DEM-Eigenschaften** aus, und klicken Sie dann auf **Datenbank-Server** | **Aktivieren**.

   Wenn die Option aktiviert ist, werden Sie benachrichtigt.

2 Klicken Sie auf **OK**, um **DEM-Eigenschaften** zu schließen.

3 Zum Anzeigen der Benachrichtigungen klicken Sie in der Systemnavigationsstruktur auf das DEM-Gerät, und wählen Sie dann Folgendes aus: **Ereignisansichten** | **Ereignisanalyse**.

4 Zum Hinzufügen des Servers zum System wählen Sie die Ansicht **Ereignisanalyse** aus, klicken Sie dann auf das Symbol **Menü**  , und wählen Sie **Server hinzufügen** aus.

Einstellungen für verteilte ESM-Geräte (DESM)

Das verteilte ESM-Gerät (DESM) verfügt über eine verteilte Architektur, über die Verbindungen zwischen dem übergeordneten ESM-Gerät und bis zu 100 Geräten möglich sind, von denen Daten gesammelt werden können. Die Daten werden durch das übergeordnete Gerät basierend auf den von Ihnen definierten Filtern vom Gerät abgerufen. Außerdem können Sie die vom Gerät stammenden Daten nahtlos aufgliedern, wobei die Daten auf dem ESM-Gerät bleiben.

Das übergeordnete ESM-Gerät muss vom DESM-Gerät genehmigt werden, damit Ereignisse abgerufen werden können. Durch das übergeordnete Gerät können Filter festgelegt, Datenquellen synchronisiert und benutzerdefinierte Typen mithilfe von Push übertragen werden. Erst nach der Genehmigung können Regeln oder Ereignisse vom DESM-Gerät abgerufen werden.

Wenn Sie sich mit Administratorrechten beim DESM-Gerät anmelden, wird die folgende Benachrichtigung angezeigt: "Dieses ESM-Gerät wurde als verteiltes ESM-Gerät auf einem anderen Server hinzugefügt. Es wird auf die Verbindung für die Genehmigung gewartet." Wenn Sie auf **Hierarchische ESM-Geräte genehmigen** klicken, können Sie den zulässigen Typ für die Kommunikation zwischen dem übergeordneten ESM-Gerät und dem DESM-Gerät auswählen.

Vom übergeordneten ESM-Gerät werden keine Geräte verwaltet, die zum ESM-Gerät gehören. Auf dem übergeordneten ESM-Gerät wird die Systemstruktur des -Geräts angezeigt, mit dem das Gerät direkt verbunden ist. Es werden keine Ereignisse von den untergeordneten ESM-Geräten der Geräte abgerufen oder angezeigt. Symbolleisten sind für alle untergeordneten DESM-Geräte deaktiviert.

Vom übergeordneten Gerät werden keine Daten verwaltet, die sich auf dem ESM-Gerät befinden. Stattdessen wird eine Teilmenge des Geräts aus den ESM-Daten übertragen und auf dem übergeordneten ESM-Gerät gespeichert. Dieser Vorgang basiert auf den von Ihnen definierten Filtern.

Hinzufügen von DESM-Filtern

Vom ESM-Gerät an das übergeordnete DESM-Gerät übertragene Daten hängen von benutzerdefinierten Filtern ab. Wenn diese Filter gespeichert werden, entspricht dies dem Anwenden des Filters auf das ESM-Gerät, damit die entsprechenden Hashes oder Bitsets generiert werden können. Da die DESM-Funktion dazu gedacht ist, Ihnen das Sammeln bestimmter Daten (nicht aller Daten) vom ESM-Gerät zu ermöglichen, müssen Sie Filter für die vom ESM-Gerät abzurufenden Daten festlegen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **DESM-Eigenschaften** aus, und klicken Sie dann auf **Filter**.

2 Geben Sie die erforderlichen Daten ein, und klicken Sie dann auf **OK**.

ePolicy Orchestrator-Einstellungen

Sie können ein ePolicy Orchestrator-Gerät zu ESM hinzufügen, dessen Anwendungen als untergeordnete Elemente in der Systemnavigationsstruktur aufgeführt werden. Nach der Authentifizierung können Sie auf Funktionen von ESM zugreifen und ePolicy Orchestrator-Tags direkt zu Quell- oder Ziel-IP-Adressen und zu durch Alarme generierten Ereignissen zuweisen.

Sie müssen ePolicy Orchestrator einem Empfänger zuordnen, da die Ereignisse nicht von ePolicy Orchestrator, sondern vom Empfänger abgerufen werden.

Sie benötigen Leseberechtigungen für die Master-Datenbank und für die ePolicy Orchestrator-Datenbank, um ePolicy Orchestrator zu verwenden.

Wenn für das McAfee ePO-Gerät ein McAfee® Threat Intelligence Exchange-Server vorhanden ist, wird dieser beim Hinzufügen des McAfee ePO-Geräts zu ESM automatisch hinzugefügt (siehe *Threat Intelligence Exchange-Integration*).

Starten von ePolicy Orchestrator

Wenn sich ein ePolicy Orchestrator-Gerät oder eine Datenquelle auf dem ESM-Gerät befindet und die IP-Adresse von ePolicy Orchestrator zum lokalen Netzwerk gehört, können Sie die Benutzeroberfläche von ePolicy Orchestrator über das ESM-Gerät starten.

Bevor Sie beginnen

Fügen Sie ein ePolicy Orchestrator-Gerät oder eine Datenquelle zum ESM-Gerät hinzu.

Diese Funktion ist in ePolicy Orchestrator 4.6 und höher verfügbar.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur eine Ansicht aus.

2 Wählen Sie in einer Balkendiagramm-, Listendiagramm-, Kreisdiagramm- oder Tabellenkomponente von der Daten zu Quell- und Ziel-IPs zurückgegeben werden, ein Ergebnis aus.

3 Klicken Sie im Menü  der Komponente auf **Aktion** | **ePO starten**.

- Wenn sich im System nur ein ePolicy Orchestrator-Gerät oder nur eine Datenquelle befindet und Sie in Schritt 1 eine Quell- oder Ziel-IP ausgewählt haben, wird ePolicy Orchestrator gestartet.
- Wenn im System mehrere ePolicy Orchestrator-Geräte oder Datenquellen vorhanden sind, wählen Sie das Gerät oder die Datenquelle aus, auf das bzw. auf die Sie zugreifen möchten. Daraufhin wird ePolicy Orchestrator gestartet.
- Wenn Sie in Schritt 1 ein Ereignis oder einen Fluss in einer Tabellenkomponente ausgewählt haben, wählen Sie aus, ob Sie auf die Quell- oder Ziel-IP-Adresse zugreifen möchten. Daraufhin wird ePolicy Orchestrator gestartet.

Authentifizierung von McAfee ePO-Geräten

Vor der Verwendung von Kennzeichnung oder Aktionen in McAfee ePO oder vor der Verwendung von McAfee Real Time for McAfee ePO ist eine Authentifizierung erforderlich.

Es gibt zwei Arten der Authentifizierung:

- Einzelnes globales Konto: Wenn Sie zu einer Gruppe gehören, die Zugriff auf ein McAfee ePO-Gerät hat, können Sie diese Funktionen nach der Eingabe globaler Anmeldeinformationen verwenden.
- Separates Konto für jedes Gerät pro Benutzer: Sie benötigen Berechtigungen zum Anzeigen des Geräts in der Gerätestruktur.

Wenn Sie Aktionen, Tags oder McAfee Real Time for McAfee ePO verwenden, müssen Sie die ausgewählte Authentifizierungsmethode verwenden. Wenn die Anmeldeinformationen nicht gefunden werden oder ungültig sind, werden Sie aufgefordert, gültige Anmeldeinformationen einzugeben. Diese müssen Sie für die zukünftige Kommunikation mit dem Gerät speichern.

Wenn Sie Berichte, Datenanreicherungen und dynamische Watchlists im Hintergrund über McAfee Real Time for McAfee ePO ausführen, werden die ursprünglich angegebenen McAfee ePO-Anmeldeinformationen verwendet.

Einrichten der Authentifizierung über ein separates Konto

Die Authentifizierung über ein globales Konto ist die Standardeinstellung. Beim Einrichten der Authentifizierung über ein separates Konto müssen Sie zwei Schritte ausführen.

1. Stellen Sie sicher, dass **Benutzerauthentifizierung erforderlich** ausgewählt ist, wenn Sie das McAfee ePO-Gerät zu ESM hinzufügen oder die Verbindungseinstellungen für das Gerät einrichten(siehe *Hinzufügen von Geräten zur ESM-Konsole* oder *Ändern der Verbindung mit ESM*).
2. Geben Sie auf der Seite **Optionen** die Anmeldeinformationen ein (siehe *Hinzufügen von Anmeldeinformationen für die McAfee ePO-Authentifizierung*).

Hinzufügen von Anmeldeinformationen für die McAfee ePO-Authentifizierung

Vor der Verwendung von Kennzeichnung oder Aktionen in McAfee ePO oder der Verwendung von McAfee Real Time for McAfee ePO müssen Sie die Anmeldeinformationen für die Authentifizierung zum ESM-Gerät hinzufügen.

Bevor Sie beginnen

Installieren Sie ein McAfee ePO-Gerät in ESM (siehe *Hinzufügen von Geräten zur ESM-Konsole*).

Wenden Sie sich an den Systemadministrator, wenn Sie den Benutzernamen und das Kennwort für das Gerät nicht kennen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf der Systemnavigationsleiste der ESM-Konsole auf **Optionen** und dann auf **ePO-Anmeldeinformationen**.
2. Klicken Sie auf das Gerät und dann auf **Bearbeiten**.
3. Geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie dann auf **Testverbindung**.
4. Klicken Sie auf **OK**.

Zuweisen von ePolicy Orchestrator-Tags zu IP-Adressen

Auf der Registerkarte **ePO-Kennzeichnung** werden die verfügbaren Tags aufgeführt. Sie können Tags durch einen Alarm generierten Ereignissen zuweisen und anzeigen, ob für einen Alarm ePolicy Orchestrator-Tags vorhanden sind. Außerdem können Sie auf dieser Seite ein oder mehrere Tags auswählen und auf eine IP-Adresse anwenden.

Für den Zugriff auf die Kennzeichnungsfunktion benötigen Sie die Berechtigungen zum **Anwenden, Ausschließen und Löschen von Tags** sowie für **Agentenreaktivierung und Anzeigen des Agenten-Aktivitätsprotokolls** in ePolicy Orchestrator.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **ePO-Eigenschaften** aus, und klicken Sie dann auf **Kennzeichnung**.
2. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **Zuweisen**.

Die ausgewählten Tags werden auf die IP-Adresse angewendet.

McAfee Risk Advisor-Datenerfassung

Sie können mehrere ePolicy Orchestrator-Server festlegen, von denen die McAfee Risk Advisor-Daten erfasst werden sollen. Die Daten werden über eine Datenbankabfrage aus der SQL Server-Datenbank von ePolicy Orchestrator erfasst.

Aus der Datenbankabfrage ergibt sich eine Liste mit einer Gegenüberstellung von IP und Reputationsfaktor. Außerdem werden Konstantenwerte für die hohen und niedrigen Reputationswerte bereitgestellt. Alle Listen aus ePolicy Orchestrator und McAfee Risk Advisor werden zusammengeführt. Dabei erhalten doppelte IPs den höchsten Faktor. Die zusammengeführte Liste wird mit den niedrigen und hohen Werten an alle ACE-Geräte gesendet, die für die Bewertung von SrcIP- und DstIP-Feldern verwendet werden.

Beim Hinzufügen von ePolicy Orchestrator werden Sie gefragt, ob Sie McAfee Risk Advisor-Daten konfigurieren möchten. Wenn Sie auf **Ja** klicken, werden eine Datenanreicherungsquelle und (gegebenenfalls) zwei ACE-Bewertungsregeln erstellt und ein entsprechender Rollout ausgeführt. Zum Anzeigen dieser Elemente wechseln Sie zu den Seiten **Datenanreicherung** und **Risikokorrelations-Bewertung**. Wenn Sie die Bewertungsregeln verwenden möchten, müssen Sie einen Risikokorrelations-Manager erstellen.

Aktivieren der McAfee Risk Advisor-Datenerfassung

Wenn Sie die McAfee Risk Advisor-Datenerfassung in ePolicy Orchestrator aktivieren, wird eine Liste mit Faktoren generiert und an alle ACE-Geräte gesendet, die für die Bewertung von SrcIP- und DstIP-Feldern verwendet werden sollen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur Folgendes aus: **ePO-Eigenschaften** | **Geräteverwaltung** aus, und klicken Sie dann auf **Aktivieren**.

   Sie werden informiert, wenn die Erfassung aktiviert ist.
2. Klicken Sie auf **OK**.

Ausführen von McAfee Real Time for McAfee ePO-Aktionen

Sie können McAfee Real Time for McAfee ePO-Aktionen für die Ergebnisse einer Frage aus ESM und der Komponente ausführen, für die in der Ansicht eine IP-Adresse angezeigt wird.

Bevor Sie beginnen

Erstellen Sie eine McAfee Real Time for McAfee ePO-Frage, und führen Sie sie aus (siehe *Abfragen von McAfee ePO für McAfee Real Time for McAfee ePO-Dashboard*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der ESM-Konsole auf das Menüsymbol  einer Ansichtskomponente, in der die Ergebnisse einer McAfee Real Time for McAfee ePO-Frage angezeigt werden.
2. Heben Sie **Aktionen** hervor, und klicken Sie dann auf **Aktionen für Real Time for ePO**.
3. Wählen Sie auf der Registerkarte **Geräte** das McAfee ePO-Gerät aus, für das Sie die Aktion ausführen möchten.
4. Klicken Sie auf der Registerkarte **Aktionen** auf eine Aktion in der Liste der für die ausgewählten Geräte verfügbaren Aktionen.
5. Legen Sie auf der Registerkarte **Filter** einen Satz von Filtern fest, die Sie auf die Frage anwenden möchten. Klicken Sie dann auf **Fertig stellen**.

Im Dashboard oder den Komponenten von McAfee ePO stehen keine Filter zur Verfügung.

Threat Intelligence Exchange-Integration

Mit Threat Intelligence Exchange wird die Reputation ausführbarer Programme auf den mit diesen Dateien verbundenen Endpunkten überprüft.

Beim Hinzufügen eines McAfee ePO-Geräts zu ESM wird automatisch erkannt, ob ein Threat Intelligence Exchange-Server mit dem Gerät verbunden ist. In diesem Fall wird DXL von ESM überwacht, und es werden Ereignisse protokolliert.

Wenn der Threat Intelligence Exchange-Server erkannt wird, werden Threat Intelligence Exchange-Watchlists, Datenanreicherung und Korrelationsregeln automatisch hinzugefügt, und Threat Intelligence Exchange-Alarme werden aktiviert. Sie erhalten eine visuelle Benachrichtigung, die einen Link zur Übersicht über die vorgenommenen Änderungen enthält. Außerdem werden Sie benachrichtigt, wenn der Threat Intelligence Exchange-Server zum McAfee ePO-Server hinzugefügt wird, nachdem das Gerät zu ESM hinzugefügt wurde.

Wenn Threat Intelligence Exchange-Ereignisse generiert wurden, können Sie den Ausführungsverlauf anzeigen (siehe *Anzeigen des Threat Intelligence Exchange-Ausführungsverlaufs und Einrichten von Aktionen*) und die Aktionen auswählen, die für die bösartigen Daten ausgeführt werden sollen.

Korrelationsregeln

Sechs Korrelationsregeln sind für Threat Intelligence Exchange-Daten optimiert. Mit diesen Regeln werden Ereignisse generiert, die Sie durchsuchen und sortieren können.

- TIE: Die GTI-Reputation wurde von Sauber in Infiziert geändert.
- TIE: Eine bösartige Datei (SHA-1) wurde auf einer steigenden Anzahl von Hosts gefunden.
- TIE: Der Name einer bösartigen Datei wurde auf einer steigenden Anzahl von Hosts gefunden.

- TIE: Auf einem einzigen Host wurden mehrere bösartige Dateien gefunden.
- TIE: Die TIE-Reputation wurde von Sauber in Infiziert geändert.
- TIE: Auf allen Hosts wurde eine Zunahme der bösartigen Dateien festgestellt.

Alarme

ESM verfügt über zwei Alarme, die ausgelöst werden können, wenn wichtige Threat Intelligence Exchange-Ereignisse erkannt werden.

- **TIE: Der Schwellenwert für ungültige Dateien ist überschritten** wird durch die Korrelationsregel **TIE: Eine bösartige Datei (SHA-1) wurde auf einer steigenden Anzahl von Hosts gefunden** ausgelöst.
- **TIE: Eine unbekannte Datei wurde ausgeführt** wird durch ein bestimmtes TIE-Ereignis ausgelöst. Dabei werden Informationen zur Watchlist für **TIE-Datenquellen-IPs** hinzugefügt.

Watchlist

In der Watchlist für **TIE-Datenquellen-IPs** werden Systeme geführt, durch die der Alarm **TIE: Eine unbekannte Datei wurde ausgeführt** ausgelöst wurde. Es handelt sich um eine statische Watchlist, die nicht abläuft.

Ausführungsverlauf für Threat Intelligence Exchange

Sie können den Ausführungsverlauf für alle Threat Intelligence Exchange-Ereignisse anzeigen (siehe *Anzeigen des Ausführungsverlaufs für Threat Intelligence Exchange und Einrichten von Aktionen*). Dazu gehört eine Liste der IP-Adressen, über die versucht wurde, die Datei auszuführen. Auf dieser Seite können Sie ein Element auswählen und die folgenden Aktionen ausführen:

- Erstellen einer neuen Watchlist
- Anfügen der Informationen an eine Watchlist
- Erstellen eines neuen Alarms
- Hinzufügen der Informationen zu einer Blacklist
- Exportieren der Informationen in eine CSV-Datei

Anzeigen des Ausführungsverlaufs für Threat Intelligence Exchange und Einrichten von Aktionen

Auf der Seite mit dem Ausführungsverlauf für Threat Intelligence Exchange wird eine Liste der Systeme angezeigt, auf denen die Datei ausgeführt wurde, die dem ausgewählten Ereignis zugeordnet ist.

> **Bevor Sie beginnen**
>
> Es muss ein ePolicy Orchestrator-Gerät vorhanden sein, mit in ESM ein Threat Intelligence Exchange-Server verbunden ist.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Systemnavigationsstruktur der ESM-Konsole auf das ePolicy Orchestrator-Gerät.
2. Wählen Sie in der Dropdown-Liste mit den Ansichten die Optionen **Ereignisansichten** | **Ereignisanalyse** aus, und klicken Sie dann auf das Ereignis.
3. Klicken Sie auf das Menüsymbol  , und wählen Sie dann die folgenden Optionen aus: **Aktionen** | **Ausführungsverlauf für TIE**.

4 Zeigen Sie auf der Seite **Ausführungsverlauf für TIE** die Systeme an, auf denen die Threat Intelligence Exchange-Datei ausgeführt wurde.

5 Zum Hinzufügen dieser Daten zu Ihrem Workflow klicken Sie auf ein System und auf das Dropdown-Menü **Aktionen**. Wählen Sie dann eine Option aus, um die zugehörige ESM-Seite zu öffnen.

6 Richten Sie die ausgewählte Aktion ein (Anweisungen finden Sie in der Online-Hilfe).

Abfragen von McAfee ePO-Geräten nach Berichten oder Ansichten

Sie können mehrere McAfee ePO-Geräte nach Berichten oder Ansichten abfragen, wenn diese in McAfee Real Time for McAfee ePO integriert sind.

Bevor Sie beginnen

Vergewissern Sie sich, dass die abzufragenden McAfee ePO-Geräte in McAfee Real Time for McAfee ePO integriert sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der Systemnavigationsstruktur auf das System, auf das Symbol **Eigenschaften**  und dann auf **Berichte**.

2 Klicken Sie auf **Hinzufügen**, füllen Sie die Abschnitte 1 bis 4 aus, und klicken Sie dann in Abschnitt 5 auf **Hinzufügen**.

3 Ziehen Sie im **Berichtslayout**-Editor eine Komponente (**Tabelle**, **Balkendiagramm** oder **Kreisdiagramm**), und legen Sie sie an der gewünschten Stelle ab.

4 Wählen Sie im **Abfragen-Assistenten** in der Dropdown-Liste die Option **Real Time for McAfee EPO** aus, und wählen Sie dann das Element oder die Frage für die Abfrage aus.

5 Klicken Sie auf **Weiter**, auf **Geräte**, und wählen Sie dann die abzufragenden McAfee ePO-Geräte aus.

6 (Optional) Klicken Sie auf **Filter**, fügen Sie die Filterwerte für die Abfrage hinzu, und klicken Sie dann auf **OK**.

7 Wenn Sie in der Dropdown-Liste die Option **Benutzerdefinierte ePO-Frage** ausgewählt haben, klicken Sie auf **Felder**, wählen Sie die Elemente aus, die in der Frage enthalten sein sollen, und klicken Sie dann auf **OK**.

8 Klicken Sie auf **Fertig stellen**, um den **Abfragen-Assistenten** zu schließen, definieren Sie im Bereich **Eigenschaften** die Eigenschaften, und speichern Sie den Bericht.

Abfragen von McAfee ePO-Geräten nach einer Datenanreicherung

Sie können mehrere McAfee ePO-Geräte nach einer Datenanreicherung abfragen, wenn diese in Real Time for McAfee ePO integriert sind.

Bevor Sie beginnen

Vergewissern Sie sich, dass die abzufragenden McAfee ePO-Geräte in McAfee Real Time for McAfee ePO integriert sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System aus. Klicken Sie auf das Symbol **Eigenschaften** und dann auf **Datenanreicherung**.
2. Klicken Sie auf **Hinzufügen**, geben Sie einen Namen ein, und treffen Sie dann auf der Registerkarte **Hauptbildschirm** eine Auswahl.
3. Wählen Sie auf der Registerkarte **Quelle** die Option McAfee Real Time for McAfee ePO im Feld **Typ** aus, und wählen Sie dann im Feld **Gerät** die Geräte aus.
4. Legen Sie die verbleibenden Einstellungen auf den Registerkarten **Abfrage**, **Bewertung** und **Ziel** fest, und klicken Sie dann auf **Fertig stellen**.

Abfragen von McAfee ePO-Geräten für das McAfee Real Time for McAfee ePO-Dashboard

Sie können in der Dashboard-Ansicht von McAfee ePO eine Abfrage für mehrere McAfee Real Time for McAfee ePO-Geräte ausführen.

> **Bevor Sie beginnen**
>
> Vergewissern Sie sich, dass die abzufragenden McAfee ePO-Geräte in McAfee Real Time for McAfee ePO integriert sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Systemnavigationsstruktur auf die abzufragenden McAfee ePO-Geräte.
2. Klicken Sie in der ESM-Konsole auf die Liste der Ansichten, und wählen Sie dann McAfee Real Time for McAfee ePO aus.
3. Wählen Sie im Bereich **Filter** die Filter aus:
   a. Klicken Sie im Abschnitt **Elemente** auf das offene Feld, und wählen Sie die Elemente für die Abfrage aus.
   b. Wählen Sie im Abschnitt **Filter** den Typ des Filters aus, und geben Sie dann den Filter in das offene Feld ein.
   c. Wählen Sie die Filteraktion aus, und geben Sie dann den Wert ein.
4. Klicken Sie auf das Symbol **Abfrage ausführen**.

Einstellungen für Nitro Intrusion Prevention System (Nitro IPS)

Mit dem McAfee Nitro Intrusion Prevention System-Gerät (Nitro IPS) können ausgeklügelte Netzwerk-Eindringungsversuche erkannt und aktiv aufgezeichnet und abgewehrt werden. Das Nitro IPS-Gerät enthält einen eingebetteten Daten-Manager (der für die Verwaltung, Datenerfassung

und Analyse sowie für erweiterte Eindringungsanalysen verwendet wird) und erweiterte Funktionen für die Analyse von Eindringungsversuchen wie beispielsweise die Erkennung von Anomalien.

Eingehende Pakete werden basierend auf einem benutzerdefinierten Regelsatz, der in einer Regelsprache nach Branchenstandard angegeben ist, selektiv weitergegeben, verworfen und protokolliert. Jedes Nitro IPS-Gerät enthält darüber hinaus eine voll funktionsfähige Firewall-Komponente, die durch Firewall-Regeln nach Branchenstandard gesteuert wird und Low-Level-Paketprüfungsfunktionen sowie ein Systemprotokoll nach Branchenstandard bereitstellt.

Assistent zur Entdeckung von Anomalien

Sie können für alle Nitro IPS-Geräte oder virtuellen Geräte auf die Entdeckung von Anomalien zugreifen. Sinnvoll ist dies jedoch nur bei Geräten, auf denen Flussdaten gesammelt wurden. Im **Assistenten zur Entdeckung von ratenbasierten Anomalien** finden Sie eine Liste und eine Beschreibung aller auf dem ausgewählten Gerät verfügbaren Variablen.

Bestimmte Firewall-Regeln basieren auf Raten. Eine ratenbasierte Regel löst nur dann eine Warnung aus, wenn der Netzwerkverkehr die Schwellenwerte überschreitet, die Sie mit Variablen aus der Firewall-Kategorie im **Richtlinien-Editor** definiert haben. Die Standardwerte für diese Variablen müssen für Ihren Netzwerkverkehr nicht zwangsläufig sinnvoll sein. Daher haben Sie im **Assistenten zur Erkennung von ratenbasierten Anomalien** die Möglichkeit, Diagramme der Netzwerk-Flussdaten in Bezug auf diese Parameter zu analysieren. Dann können Sie die Standardwerte auswählen, einen eigenen Wert festlegen oder auswählen, dass die Daten vom ESM-Gerät analysiert werden und dabei geschätzt wird, welche Werte basierend auf dem Verlauf des Datenverkehrs im Netzwerk am besten geeignet sind. Jedes Netzwerk ist anders. Daher sollten Sie sich mit dem Verlauf des Datenverkehrs vertraut machen, indem Sie diese visuellen Analyseberichte überprüfen und die für Ihre Anforderungen geeigneten Werte auswählen.

Über den Assistenten werden viele komplizierte Berechnungen ausgeführt, um die vorgeschlagenen Werte zu ermitteln und eine visuelle Analyse der Muster des Netzwerkverkehrs anzuzeigen. Wenn in Nitro IPS, auf dem virtuellen Gerät, auf dem Empfänger und in der Datenquelle eine große Menge von Flussdaten vorhanden ist, sollten Sie den Zeitbereich für diese Berechnungen begrenzen. Verwenden Sie ein paar Tage oder eine Woche mit normaler Netzwerkaktivität als Basislinie für die Berechnung der Werte. Wenn Sie einen längeren Zeitraum verwenden, beanspruchen die Berechnungen möglicherweise zu viel Zeit.

Hier ist eine Liste mit den Firewall-Regeln für ratenbasierte Anomalien und den Variablen, die sich auf die Funktionsweise der Regeln auswirken:

Regel	Variablen
Large inbound byte rate	LARGE_INBOUND_BYTE_RATE_LIMIT, LARGE_INBOUND_BYTE_RATE_SECONDS
Large inbound bytes	LARGE_INBOUND_BYTES_LIMIT
Large inbound network connections rate	LARGE_IB_CONN_RATE_BURST, LARGE_IB_CONN_RATE_LIMIT
Large inbound packet rate	LARGE_INBOUND_PACKET_RATE_LIMIT, LARGE_INBOUND_PACKET_RATE_SECS
Large inbound packet	LARGE_INBOUND_PACKETS_LIMIT
Large outbound byte rate	LARGE_OUTBOUND_BYTE_RATE_LIMIT, LARGE_OUTBOUND_BYTE_RATE_SECONDS
Large outbound network connection rate	LARGE_OB_CONN_RATE_BURST, LARGE_OB_CONN_RATE_LIMIT
Large outbound packet rate	LARGE_OUTBOUND_PACKET_RATE_LIMIT, LARGE_OUTBOUND_PACKET_RATE_SECS

Regel	Variablen
Large outbound packets	LARGE_OUTBOUND_PACKETS_LIMIT
Long connection duration	LONG_DURATION_SECONDS

Bearbeiten von Variablen für die Entdeckung von Anomalien

Im **Assistenten zur Entdeckung von ratenbasierten Anomalien** werden die Variablen für die Entdeckung von Anomalien aufgeführt. Außerdem finden Sie hier verschiedene Optionen, die Sie zum Analysieren der Daten aus der Entdeckung von ratenbasierten Anomalien verwenden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Nitro IPS-Gerät oder ein virtuelles Gerät aus, auf dem Flussdaten gesammelt wurden. Klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie im Feld **Assistent zur Entdeckung von Anomalien** auf **Bearbeiten**.
3. Führen Sie eine oder mehrere der verfügbaren Funktionen aus, und klicken Sie dann auf **OK**.

Generieren eines Analyseberichts

Der **Analysebericht** enthält eine visuelle Analyse verschiedener Aspekte des Netzwerkverkehrs.

Dieser Bericht ist hilfreich, wenn Sie sich einen visuellen Eindruck von den Verkehrsmustern im Netzwerk verschaffen möchten. Die gesammelten Daten können Ihnen Entscheidungen bei der Auswahl von Werten für die Regelparameter für ratenbasierte Anomalien erleichtern.

Damit Sie einen Bericht generieren können, müssen auf dem Gerät mindestens 10.000 generierte Flüsse vorhanden sein.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Nitro IPS-Gerät aus, auf dem Flussdaten gesammelt wurden. Klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie im Feld **Assistent zur Entdeckung von Anomalien** auf **Bearbeiten**.
3. Klicken Sie auf **Analyse** | **Analysebericht**, und wählen Sie dann den Zeitbereich und die Variable für den Bericht aus.
4. Klicken Sie auf **OK**.

Der Bericht wird generiert. Sie können die vertikale und die horizontale Skala vergrößern oder verkleinern, indem Sie gegebenenfalls auf die runden Symbole an den Diagrammachsen klicken und diese an die gewünschte Stelle ziehen.

Zugreifen auf Firewall-Regeln und Standardregeln

Regeln werden im **Richtlinien-Editor** hinzugefügt und verwaltet. Sie können jedoch Firewall-Regeln und Standardregeln von den IPS-Geräten oder virtuellen IPS-Geräten lesen, schreiben, anzeigen, exportieren und importieren.

Die Regeln sollten nicht regelmäßig über diese Seite verwaltet werden. Wenn Sie die Regeln auf diese Weise ändern, werden die Richtlinieneinstellungen des Geräts nicht mit den Einstellungen im **Richtlinien-Editor** synchronisiert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **IPS-Eigenschaften** aus, und klicken Sie dann auf **Firewall-Regeln** oder **Standardregeln**.

2 Wählen Sie eine der Optionen aus, und klicken Sie dann auf **OK**.

Blacklist für IPS oder virtuelles Gerät

Mit der Blacklist blockieren Sie durch das Gerät fließenden Datenverkehr vor der Analyse durch das Modul für die gründliche Paketprüfung.

Mit dem **Blacklist-Editor** können Sie blockierte Quellen, blockierte Ziele und Ausschlusseinstellungen für das Gerät verwalten. Außerdem können Sie auswählen, ob die Einstellungen unter **Globale Blacklist** für das Gerät gelten sollen. Wenn die Einstellungen für das Gerät gelten sollen, müssen Sie oben im Editor das Kontrollkästchen **Globale Blacklist einschließen** aktivieren.

Der Bildschirm **Blacklist-Editor** enthält drei Registerkarten:

- **Blockierte Quellen**: Ermittelt Übereinstimmungen mit der Quell-IP-Adresse des durch das Gerät geleiteten Datenverkehrs.
- **Blockierte Ziele**: Ermittelt Übereinstimmungen mit der Ziel-IP-Adresse des durch das Gerät geleiteten Datenverkehrs.
- **Ausschlüsse**: Verhindert, dass Datenverkehr automatisch zu einer der Blacklists hinzugefügt wird. Kritische IP-Adressen (z. B. DNS-Server und andere Server oder die Arbeitsstationen von Systemadministratoren) können zu den Ausschlüssen hinzugefügt werden. Dann ist sichergestellt, dass diese ungeachtet der von ihnen generierten Ereignisse nie automatisch in die Blacklist aufgenommen werden.

Sie können Einträge sowohl auf der Registerkarte **Blockierte Quellen** als auch auf der Registerkarte **Blockierte Ziele** konfigurieren, um die Auswirkungen der Blacklist auf einen bestimmten Ziel-Port einzuschränken.

Hosts können auch manuell zur Blacklist hinzugefügt oder daraus entfernt werden. Wenn eine der Registerkarten im **Blacklist-Editor** ausgewählt ist, können Sie einen Eintrag hinzufügen oder ändern. Beim Hinzufügen eines Eintrags sind unter anderem die Felder **IP-Adresse**, **Port** (Version 6.2.X und höher) und **Dauer** (dauerhaft oder temporär) erforderlich. Außerdem ist das optionale Feld **Beschreibung** vorhanden.

Berücksichtigen Sie beim Hinzufügen von Einträgen Folgendes:

- **Hinzufügen** und **Ändern** werden abhängig von den geänderten Informationen aktiviert. Beim Ändern der IP-Adresse oder des Ports wird **Hinzufügen** aktiviert. Wenn Sie Dauer oder Beschreibung ändern, wird **Ändern** aktiviert.
- Einträge in den Listen **Blockierte Quellen** und **Blockierte Ziele** können so konfiguriert werden, dass Quellen oder Ziele für alle Ports oder für einen bestimmten Port in die Blacklist aufgenommen werden.
- Beim Konfigurieren von Einträgen mit einem maskierten IP-Adressbereich müssen Sie den Port auf **Alle** (0) und die Dauer auf Dauerhaft festlegen.

- Einträge können temporär (in Minuten, Stunden oder Tagen) oder dauerhaft hinzugefügt werden. Einträge unter **Ausschlüsse** müssen jedoch dauerhaft sein.
- Für diese Listen ist zwar das IP-Adressformat erforderlich, aber es ist ein Tool enthalten, mit dem die Adressen verständlicher gestaltet werden können. Wenn Sie eine IP-Adresse oder einen Host-Namen in das Feld **IP-Adresse** eingegeben haben, wird neben diesem Steuerelement abhängig vom eingegebenen Wert die Schaltfläche **Auflösen** oder **Suche** angezeigt. Wenn Sie **Auflösen** auswählen, wird der eingegebene Host-Name aufgelöst, das Feld **IP-Adresse** wird mit diesen Informationen ausgefüllt, und der Host-Name wird in das Feld **Beschreibung** verschoben. Wenn Sie **Suche** auswählen, wird eine Suche nach der IP-Adresse ausgeführt, und das Feld **Beschreibung** wird mit den Ergebnissen der Suche ausgefüllt. Manche Websites haben mehrere oder wechselnde IP-Adressen. Daher können Sie sich bei einigen Websites nicht darauf verlassen, dass sie mit diesem Tool zuverlässig blockiert werden.

Sie können IP-Adressen in der Liste auswählen und von ihnen generierte Ereignisse in einem Zusammenfassungsbericht anzeigen. Auf diese Weise können Sie die Ereignisse sehen, die von den Angreifern ausgelöst wurden, Ereignisse, die zur Blacklist hinzugefügt wurden, oder andere Angriffe, die möglicherweise vor der Aufnahme in die Blacklist eingeleitet wurden.

Im **Blacklist-Editor** können Sie außerdem Ereignisse anwenden, erneut laden und entfernen.

Verwalten der IPS-Blacklist

Sie können die IPS-Blacklist im **Blacklist-Editor** verwalten. Sie können Elemente hinzufügen, ändern oder löschen, Änderungen in die Blacklist schreiben, neue und aktualisierte Informationen vom Gerät lesen, von den angreifenden IP-Adressen generierte Ereignisse anzeigen und Hostnamen oder IP-Adressen suchen oder auflösen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **IPS-Eigenschaften** aus, und klicken Sie dann auf **Blacklist** | **Editor**.
2. Wählen Sie die Registerkarte **Blockierte Quellen**, **Blockierte Ziele** oder **Ausschlüsse** aus.
3. Führen Sie die gewünschten Aktionen aus, und klicken Sie dann auf **Schließen**.

Konfigurieren der automatischen Aufnahme in die Blacklist

Auf der Seite **Einstellungen für die automatische Aufnahme in die Blacklist** können Sie die Konfigurationseinstellungen für die automatische Aufnahme in die Blacklist für das Gerät verwalten.

Die automatische Aufnahme in die Blacklist wird pro Gerät konfiguriert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **IPS-Eigenschaften** aus, und klicken Sie dann auf **Blacklist** | **Einstellungen**.
2. Definieren Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **OK**.

McAfee Vulnerability Manager-Einstellungen

McAfee Vulnerability Manager kann als Gerät zu ESM hinzugefügt werden, sodass Sie einen Scan in McAfee Vulnerability Manager über das ESM-Gerät starten können. Dies ist hilfreich, wenn Sie ein McAfee Vulnerability Manager-Gerät erworben haben, das Sie über das ESM-Gerät ausführen möchten.

McAfee Vulnerability Manager muss einem Empfänger zugeordnet sein, da die Ereignisse nicht von McAfee Vulnerability Manager, sondern vom Empfänger abgerufen werden.

Abrufen des Zertifikats und der Passphrase für McAfee Vulnerability Manager

Sie müssen das Zertifikat und die Passphrase für McAfee Vulnerability Manager abrufen, bevor Sie McAfee Vulnerability Manager-Verbindungen einrichten. Diese Aufgabe führen Sie nicht auf dem ESM-Gerät aus.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Führen Sie auf dem Server mit Foundstone Certificate Manager die Datei Foundstone Certificate Manager.exe aus.
2. Klicken Sie auf die Registerkarte **SSL-Zertifikate erstellen**.
3. Geben Sie in das Feld **Host-Adresse** den Hostnamen oder die IP-Adresse für das System ein, auf dem die Web-Benutzeroberfläche für McAfee Vulnerability Manager gehostet wird. Klicken Sie dann auf **Auflösen**.
4. Klicken Sie auf **Zertifikat mit allgemeinem Namen erstellen**, um die Passphrase und eine ZIP-Datei zu generieren.
5. Laden Sie die ZIP-Datei hoch, und kopieren Sie die generierte Passphrase.

Ausführen von McAfee Vulnerability Manager-Scans

Auf der Seite **Scans** werden alle zurzeit oder zu einem früheren Zeitpunkt von McAfee Vulnerability Manager ausgeführten Schwachstellen-Scans und deren Status angezeigt. Wenn Sie diese Seite öffnen, wird durch eine API überprüft, ob standardmäßige Web-Anmeldeinformationen vorhanden sind. Wenn dies der Fall ist, wird die Scan-Liste basierend auf diesen Anmeldeinformationen ausgefüllt und alle 60 Sekunden aktualisiert. Außerdem können Sie über diese Seite einen neuen Scan initiieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **MVM-Eigenschaften** aus, und klicken Sie dann auf **Scans**.
2. Klicken Sie auf **Neuer Scan**, und geben Sie die erforderlichen Informationen ein.
3. Klicken Sie auf **OK**.

Nach Abschluss des Scans wird dieser zur Liste der Scans hinzugefügt.

Einrichten der McAfee Vulnerability Manager-Verbindung

Sie müssen McAfee Vulnerability Manager-Verbindungen mit der Datenbank einrichten, um die Vulnerability Assessment-Daten aus McAfee Vulnerability Manager abzurufen, und mit der Web-Benutzeroberfläche, um Scans in McAfee Vulnerability Manager auszuführen.

> **Bevor Sie beginnen**
> Sie müssen das Zertifikat und die Passphrase für McAfee Vulnerability Manager abrufen.

Wenn Sie diese Einstellungen ändern, hat dies keine Auswirkungen auf das Gerät selbst. Die Änderungen wirken sich nur auf die Kommunikation zwischen dem Gerät und ESM aus.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **MVM-Eigenschaften** aus, und klicken Sie dann auf **Verbindung**.
2. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

McAfee Network Security Manager-Einstellungen

Sie können McAfee Network Security Manager als Gerät zu ESM hinzufügen, sodass Sie über ESM auf die Funktionen zugreifen können. Dies ist hilfreich, wenn Sie ein Gerät erworben haben, auf das Sie über ESM zugreifen möchten.

Wenn Sie ein McAfee Network Security Manager-Gerät zu ESM hinzufügen, werden die Sensoren des Geräts in der Systemnavigationsstruktur unter dem Gerät als untergeordnete Elemente aufgeführt. Das Gerät muss einem Empfänger zugeordnet sein, da die Ereignisse nicht von McAfee Network Security Manager, sondern vom Empfänger abgerufen werden.

Hinzufügen eines Blacklist-Eintrags

Die Anwendung der Blacklist durch McAfee Network Security Manager erfolgt über die Sensoren. Auf der Seite **Blacklist** werden die Blacklist-Einträge angezeigt, die für den ausgewählten Sensor definiert wurden. Über diese Seite können Sie Blacklist-Elemente hinzufügen, bearbeiten und löschen.

Sie müssen Superuser sein, damit Sie die Blacklist-Funktion verwenden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **NSM-Eigenschaften** aus, klicken Sie auf **Blacklist**, und wählen Sie dann einen Sensor aus.
2. Zum Anwenden der Einträge in der globalen Blacklist auf den Sensor wählen Sie **Globale Blacklist einschließen** aus.

   Das Element der globalen Blacklist wird zur Liste hinzugefügt. Bei doppelten IP-Adressen wird die Adresse von McAfee Network Security Manager mit der Adresse aus der globalen Blacklist überschrieben.

   Die Auswahl dieser Option kann nicht automatisch rückgängig gemacht werden. Sie müssen die Elemente manuell löschen.

3. Klicken Sie auf **Hinzufügen**, geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Der Eintrag wird bis zum Ablauf der Dauer in der Blacklist angezeigt.

Hinzufügen oder Löschen eines entfernten Blacklist-Eintrags

Für Einträge, die auf dem ESM-Gerät mit einer nicht abgelaufenen Dauer initiiert wurden, die aber beim Abfragen von McAfee Network Security Manager (Manager) nicht in der Liste der Blacklist-Einträge zurückgegeben werden, wird der Status **Entfernt** und ein Kennzeichnungssymbol angezeigt.

Diese Bedingung tritt auf, wenn der Eintrag entfernt wurde, ohne dass das Entfernen auf dem ESM-Gerät initiiert wurde. Sie können den Eintrag erneut hinzufügen oder ihn aus der Blacklist löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **NSM-Eigenschaften** aus, und klicken Sie dann auf **Blacklist**.
2. Wählen Sie in der Liste der Blacklist-Einträge den entfernten Eintrag aus, und klicken Sie dann auf **Hinzufügen** oder **Löschen**.
3. Klicken Sie auf **Anwenden** oder **OK**.

Konfigurieren von zusätzlichen Diensten

Zu den zusätzlichen Diensten gehören Remedy-Server, NTP-Server (Network Time Protocol) und DNS-Server. Konfigurieren Sie diese Server für die Kommunikation mit ESM.

Inhalt

- *Allgemeine Systeminformationen*
- *Konfigurieren von Remedy-Server-Einstellungen*
- *Definieren von Nachrichteneinstellungen*
- *Einrichten von NTP auf einem Gerät*
- *Konfigurieren von Netzwerkeinstellungen*
- *Systemzeitsynchronisierung*
- *Installieren eines neuen Zertifikats*
- *Konfigurieren von Profilen*
- *SNMP-Konfiguration*

Allgemeine Systeminformationen

Auf der Seite **Systemeigenschaften** | **Systeminformationen** sehen Sie allgemeine Informationen zum System und den Status der verschiedenen Funktionen. Auf der Seite **Systemprotokoll** sehen Sie Ereignisse, die im System oder auf den Geräten aufgetreten sind.

Diese Informationen können Sie heranziehen, wenn Sie mit dem McAfee-Support über Ihr System sprechen, Funktionen wie Ereignis- oder Flussaggregation einrichten oder den Status einer Regelaktualisierung oder einer Systemsicherung überprüfen.

- Unter **System**, **Kunden-ID**, **Hardware** und **Seriennummer** finden Sie Informationen zum System und zu seinem aktuellen Betriebsstatus.
- **Datenbankstatus** wird angezeigt, wenn in der Datenbank andere Funktionen ausgeführt werden (z. B. eine erneute Erstellung der Datenbank oder eine erneute Erstellung im Hintergrund). Der Status dieser Funktion wird ebenfalls angezeigt. Der Status **OK** bedeutet, dass die Datenbank normal funktioniert.
- Unter **Systemuhr** werden Datum und Uhrzeit des Zeitpunkts angezeigt, an dem die **Systemeigenschaften** letztmals geöffnet oder aktualisiert wurden.
- Unter **Regelaktualisierung**, **Ereignisse**, **Flüsse und Protokolle** und **Sichern und wiederherstellen** wird angezeigt, wann letztmals die Regeln aktualisiert wurden, Ereignisse, Flüsse und Protokolle abgerufen wurden und eine Sicherung und Wiederherstellung ausgeführt wurde.

- Beim Betrieb im FIPS-Modus werden unter **FIPS-Selbsttest** und **Status** Zeitpunkt und Status des letzten FIPS-Selbsttests angezeigt.
- Unter **Berichte anzeigen** werden die Berichte **Anzahl der Gerätetypen** und **Ereigniszeitpunkt** angezeigt.

Konfigurieren von Remedy-Server-Einstellungen

Wenn ein Remedy-System eingerichtet ist, müssen Sie die Remedy-Einstellungen so konfigurieren, dass die Kommunikation zwischen dem ESM-Gerät und dem Remedy-System möglich ist.

Bevor Sie beginnen
Richten Sie das Remedy-System ein.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Benutzerdefinierte Einstellungen** | **Remedy**.
2. Geben Sie auf der Seite **Remedy-Konfiguration** die Informationen für das Remedy-System ein, und klicken Sie dann auf **OK**.

Wenn Sie in der Ansicht **Ereignisanalyse**  die Option **Ereignis an Remedy senden** auswählen, wird die E-Mail mit den auf dieser Seite eingegebenen Informationen ausgefüllt.

Definieren von Nachrichteneinstellungen

Wenn Sie die Aktionseinstellungen für einen Alarm definieren oder die Zustellungsmethode für einen Bericht einrichten, können Sie auswählen, dass eine Nachricht gesendet werden soll. Dazu müssen Sie das ESM-Gerät mit dem E-Mail-Server verbinden und die Empfänger konfigurieren, an die Sie E-Mail-, SMS-, SNMP- oder Syslog-Nachrichten senden möchten.

Alarmbenachrichtigungen können über das Protokoll SNMP v1 gesendet werden. Bei SNMP wird UDP (User Datagram Protocol) als Transportprotokoll für die Übergabe von Daten zwischen Managern und Agenten verwendet. In einer typischen SNMP-Konfiguration können von einem Agenten wie dem ESM-Gerät Ereignisse an einen (normalerweise als Netzwerkverwaltungsstation [Network Management Station, NMS] bezeichneten) SNMP-Server weitergeleitet werden. Dabei werden Datenpakete verwendet, die als Traps bezeichnet werden. Dies kann hilfreich sein, wenn Sie Ereignisberichte vom ESM-Gerät auf die gleiche Weise wie Benachrichtigungen von anderen Agenten im Netzwerk erhalten möchten. Aufgrund der Größenbeschränkungen der SNMP-Trap-Pakete wird jede Zeile des Berichts in einem separaten Trap gesendet.

Vom ESM-Gerät generierte CSV-Abfrageberichte können auch über Syslog gesendet werden. Die CSV-Abfrageberichte werden in einer Zeile pro Syslog-Nachricht gesendet. Die Daten der einzelnen Zeilen der Abfrageergebnisse sind in durch Kommas getrennten Feldern angeordnet.

Verbinden mit dem E-Mail-Server

Konfigurieren Sie die Einstellungen für die Verbindung mit Ihrem E-Mail-Server, damit Sie Nachrichten im Zusammenhang mit Alarmen und Berichten senden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, klicken Sie auf **E-Mail-Einstellungen**, und geben Sie den Host und den Port für den E-Mail-Server ein.
2. Geben Sie die erforderlichen Informationen für die Verbindung mit dem E-Mail-Server ein.
3. Klicken Sie auf **Anwenden** oder **OK**, um die Einstellungen zu speichern.

Siehe auch

Verwalten von Empfängern auf Seite 179

Verwalten von Empfängern

Alarm- oder Berichtnachrichten können in verschiedenen Formaten gesendet werden, für die Sie jeweils eine Empfängerliste verwalten können. Sie können die E-Mail-Adressen gruppieren, damit Sie Nachrichten an mehrere Empfänger gleichzeitig senden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **E-Mail-Einstellungen**.
2. Klicken Sie auf **Empfänger konfigurieren**, und wählen Sie dann die Registerkarte aus, zu der Sie die Empfänger hinzufügen möchten.
3. Klicken Sie auf **Hinzufügen**, und fügen Sie dann die erforderlichen Informationen hinzu.
4. Klicken Sie auf **OK**.

Der Empfänger wird zum ESM-Gerät hinzugefügt, und Sie können ihn überall dort auf dem ESM-Gerät auswählen, wo Empfänger verwendet werden.

Einrichten von NTP auf einem Gerät

Synchronisieren Sie die Gerätezeit über einen NTP-Server (Network Time Protocol) mit ESM.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Konfiguration** | **NTP**.
3. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Aufgaben

- *Anzeigen des Status von NTP-Servern* auf Seite 180
  Zeigen Sie den Status aller NTP-Server auf dem ESM-Gerät an.

Anzeigen des Status von NTP-Servern

Zeigen Sie den Status aller NTP-Server auf dem ESM-Gerät an.

Bevor Sie beginnen

Fügen Sie zu ESM oder den Geräten NTP-Server hinzu (siehe *Systemzeitsynchronisierung* oder *Einrichten von NTP auf einem Gerät*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Führen Sie in der Systemnavigationsstruktur einen der folgenden Schritte aus:

- Wählen Sie Folgendes aus: **Systemeigenschaften** | **Systeminformationen**aus, und klicken Sie dann auf **Systemuhr**.
- Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, klicken Sie auf das Symbol **Eigenschaften**, und wählen Sie dann Folgendes aus: **Konfiguration** | **NTP**.

2 Klicken Sie auf **Status**, zeigen Sie die Daten für den NTP-Server an, und klicken Sie dann auf **Schließen**.

Siehe auch

Systemzeitsynchronisierung auf Seite 186
Einrichten von NTP auf einem Gerät auf Seite 43

Konfigurieren von Netzwerkeinstellungen

Konfigurieren Sie, wie die Verbindung zwischen ESM und dem Netzwerk hergestellt wird, indem Sie IP-Adressen für das ESM-Server-Gateway und DNS-Server hinzufügen, Proxyserver-Einstellungen definieren, SSH einrichten und statische Routen hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Netzwerkeinstellungen**.

2 Geben Sie die Informationen zum Konfigurieren der Verbindung mit dem Netzwerk ein.

3 Klicken Sie auf **Anwenden** oder **OK**.

Aufgaben

- *Einrichten des IPMI-Ports in ESM oder auf Geräten* auf Seite 183
  Konfigurieren Sie das Netzwerk für den IPMI-Port, um IPMI in ESM oder auf den zugehörigen Geräten einzurichten.
- *Einrichten der Steuerung des Netzwerkverkehrs in ESM* auf Seite 184
  Definieren Sie einen Höchstwert für die Datenausgabe für ESM.
- *Einrichten von DHCP* auf Seite 185
  Mithilfe von DHCP (Dynamic Host Configuration Protocol) werden in IP-Netzwerken Konfigurationsparameter wie beispielsweise IP-Adressen für Schnittstellen und Dienste dynamisch verteilt.
- *Einrichten von DHCP in einem VLAN* auf Seite 186
  Mithilfe von DHCP (Dynamic Host Configuration Protocol) werden in IP-Netzwerken Konfigurationsparameter wie beispielsweise IP-Adressen für Schnittstellen und Dienste dynamisch verteilt.

Verwalten von Netzwerkschnittstellen

Die Kommunikation mit einem Gerät kann über die öffentlichen und privaten Schnittstellen der Datenverkehrspfade erfolgen. Dies bedeutet, dass das Gerät im Netzwerk nicht sichtbar ist, da es keine IP-Adresse benötigt.

Verwaltungsschnittstelle

Netzwerkadministratoren können alternativ eine Verwaltungsschnittstelle mit einer IP-Adresse für die Kommunikation zwischen ESM und dem Gerät konfigurieren. Für die folgenden Funktionen eines Geräts muss eine Verwaltungsschnittstelle verwendet werden:

- Vollständige Kontrolle über Umgehungs-Netzwerkkarten
- Verwenden der Zeitsynchronisierung über NTP
- Vom Geräten generiertes Syslog
- SNMP-Benachrichtigungen

Geräte sind mit mindestens einer Verwaltungsschnittstelle ausgestattet, über die das Gerät eine IP-Adresse erhält. Mit einer IP-Adresse ist der direkte Zugriff auf das Gerät durch ESM möglich, ohne dass die Kommunikation an eine andere Ziel-IP-Adresse oder einen anderen Hostnamen geleitet werden muss.



Verbinden Sie die Verwaltungsschnittstelle des Netzwerks nicht mit einem öffentlichen Netzwerk, da sie dann für das öffentliche Netzwerk sichtbar ist und ihre Sicherheit kompromittiert werden kann.

Bei einem Gerät im Nitro IPS-Modus benötigen Sie für jeden Pfad des Netzwerkverkehrs zwei Schnittstellen. Für den IDS-Modus sind mindestens zwei Netzwerkschnittstellen im Gerät erforderlich. Sie können im Gerät mehrere Verwaltungsschnittstellen für das Netzwerk konfigurieren.

Umgehungs-Netzwerkkarte

Für ein Gerät im Umgehungsmodus wird sämtlicher Verkehr zugelassen, auch bösartiger Datenverkehr. Unter normalen Umständen kann es ein bis drei Sekunden lang zu einem Verbindungsverlust kommen, wenn das Gerät in den Umgehungsmodus wechselt. Beim Verlassen des Umgehungsmodus kann die Verbindung für 18 Sekunden getrennt werden. Bei Verbindungen mit bestimmten Switches, beispielsweise einigen Modellen von Cisco Catalyst, sind andere Zahlen möglich. In diesem Fall kann die Verbindung 33 Sekunden lang getrennt werden, wenn das Gerät in den Umgehungsmodus wechselt oder diesen verlässt.

In dem Szenario, in dem es 33 Sekunden dauert, die Kommunikation wieder herzustellen, können Sie Portfast für den Switch-Port aktivieren und die Geschwindigkeit sowie den Duplex-Modus manuell festlegen, um wieder normale Zeiten zu erzielen. Achten Sie darauf, für alle vier Ports (Switch, beide Ports von Nitro IPS und den Port des anderen Geräts) die gleiche Einstellung festzulegen. Anderenfalls tritt möglicherweise im Umgehungsmodus ein Aushandlungsproblem auf (siehe *Einrichten von Umgehungs-Netzwerkkarten*).

Die verfügbaren Umgehungsoptionen hängen vom Typ der Umgehungs-Netzwerkkarte im Gerät ab (Typ 2 oder Typ 3).

Einrichten von Netzwerkschnittstellen

Mit Schnittstelleneinstellungen bestimmen Sie, wie die Verbindung zwischen ESM und dem Gerät hergestellt wird. Sie müssen diese Einstellungen für jedes Gerät definieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie für das Gerät auf die Option **Konfiguration** und dann auf **Schnittstellen**.
3. Geben Sie die erforderlichen Daten ein, und klicken Sie dann auf **Anwenden**.

Alle Änderungen werden mithilfe von Push an das Gerät übertragen und werden sofort wirksam. Beim Anwenden der Änderungen wird das Gerät erneut initialisiert, wodurch alle aktuellen Sitzungen getrennt werden.

Hinzufügen von VLANs und Aliassen

Fügen Sie virtuelle lokale Netzwerke (Virtual Local Area Networks, VLANs) und Aliasse (zugewiesene Paare aus IP-Adresse und Netzmaske, die Sie hinzufügen, wenn Sie ein Netzwerkgerät mit mehreren IP-Adressen haben) zu einer ACE- oder ELM-Schnittstelle hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf die Geräteoption **Konfiguration**, auf **Schnittstellen** und dann auf **Erweitert**.
3. Klicken Sie auf **VLAN hinzufügen**, geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.
4. Wählen Sie das VLAN aus, zu dem Sie den Alias hinzufügen möchten, und klicken Sie dann auf **Alias hinzufügen**.
5. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Hinzufügen von statischen Routen

Bei einer statischen Route handelt es sich um einen Satz von Anweisungen, aus denen hervorgeht, wie Hosts oder Netzwerke erreicht werden können, die nicht über das Standard-Gateway verfügbar sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Konfiguration** | **Schnittstellen**.
3. Klicken Sie neben der Tabelle **Statische Routen** auf **Hinzufügen**.
4. Geben Sie die Informationen ein, und klicken Sie dann auf **OK**.

Umgehungs-Netzwerkkarte

Unter normalen Umständen kann es ein bis drei Sekunden lang zu einem Verbindungsverlust kommen, wenn das Gerät in den Umgehungsmodus wechselt. Beim Verlassen des Umgehungsmodus kann die Verbindung für 18 Sekunden getrennt werden. Bei Verbindungen mit bestimmten Switches,

beispielsweise einigen Modellen von Cisco Catalyst, sind andere Zahlen möglich. In diesem Fall kann die Verbindung 33 Sekunden lang getrennt werden, wenn das Gerät in den Umgehungsmodus wechselt oder diesen verlässt.

In dem Szenario, in dem es 33 Sekunden dauert, die Kommunikation wieder herzustellen, können Sie Portfast für den Switch-Port aktivieren und die Geschwindigkeit sowie den Duplex-Modus manuell festlegen, um wieder normale Zeiten zu erzielen. Achten Sie darauf, für alle vier Ports (Switch, beide Ports von Nitro IPS und den Port des anderen Geräts) die gleiche Einstellung festzulegen. Anderenfalls tritt möglicherweise im Umgehungsmodus ein Aushandlungsproblem auf.

Die verfügbaren Umgehungsoptionen hängen vom Typ der Umgehungs-Netzwerkkarte im Gerät ab (Typ 2 oder Typ 3).

Einrichten von Umgehungs-Netzwerkkarten

Auf IPS-Geräten können Sie Einstellungen für eine Umgehungs-Netzwerkkarte definieren, um sämtlichen Verkehr passieren zu lassen.

ADM-und DEM-Geräte befinden sich immer im IDS-Modus. Sie können Typ und Status der Umgehungs-Netzwerkkarte anzeigen, aber Sie können die Einstellungen nicht ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Konfiguration** | **Schnittstellen**.
3. Wechseln Sie auf der Seite **Einstellungen für Netzwerkschnittstellen** unten zum Abschnitt **Konfiguration für Umgehungs-Netzwerkkarte**.
4. Sie können Typ und Status anzeigen oder auf einem IPS-Gerät die Einstellungen ändern.
5. Klicken Sie auf **OK**.

Einrichten des IPMI-Ports in ESM oder auf Geräten

Sie können den IPMI-Port in ESM oder den zugehörigen Geräten einrichten.

Auf diese Weise können Sie verschiedene Aktionen ausführen:

- Schließen Sie die IPMI-Netzwerkkarte (Network Interface Controller, NIC) an einen Switch an, damit sie für IPMI-Software verfügbar ist.
- Greifen Sie auf eine IPMI-basierte Kernel-basierte virtuelle Maschine (Kernel-Based Virtual Machine, KVM) zu.
- Legen Sie nach dem Upgrade auf ESM 9.4.0 das IPMI-Kennwort für den Standardbenutzer fest.
- Greifen Sie auf IPMI-Befehle zu, beispielsweise zum Einschalten und zum Abfragen des Energiestatus.
- Setzen Sie die IPMI-Karte zurück.
- Führen Sie warme und kalte Zurücksetzungen aus.

Einrichten des IPMI-Ports in ESM oder auf Geräten

Konfigurieren Sie das Netzwerk für den IPMI-Port, um IPMI in ESM oder auf den zugehörigen Geräten einzurichten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System oder eines der Geräte aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Greifen Sie auf die Registerkarte **Netzwerkeinstellungen Erweitert** zu.

- Klicken Sie in ESM auf **Netzwerkeinstellungen** | **Erweitert**.
- Klicken Sie auf einem Gerät auf die Option **Konfiguration** für das Gerät und dann auf **Schnittstellen** | **Erweitert**

3 Wählen Sie **IPMI-Einstellungen aktivieren** aus, und geben Sie dann VLAN, IP-Adresse, Netzmaske und Gateway für die IPMI-Karte ein.

Wenn **IPMI-Einstellungen aktivieren** im Geräte-BIOS abgeblendet ist, müssen Sie das System-BIOS aktualisieren. Stellen Sie eine SSH-Verbindung mit dem Gerät her, und öffnen Sie die Datei `/etc/areca/system_bios_update/Contents-README.txt`.

4 Klicken Sie auf **Anwenden** oder **OK**.

Wenn Sie ein Upgrade für das Gerät durchführen, werden Sie möglicherweise in einer Meldung informiert, dass Sie das Kennwort ändern oder den Authentifizierungsschlüssel für das Gerät erneut festlegen müssen. Wenn diese Meldung angezeigt wird, ändern Sie das Systemkennwort, oder legen Sie den Authentifizierungsschlüssel für das Gerät erneut fest, um ein neues Kennwort zum Konfigurieren von IPMI festzulegen.

Einrichten der Steuerung des Netzwerkverkehrs in ESM

Definieren Sie einen Höchstwert für die Datenausgabe für ESM.

Diese Funktion ist hilfreich, wenn Einschränkungen für die Bandbreite gelten und Sie die Menge der Daten steuern möchten, die von den einzelnen ESM-Geräten gesendet werden können. Dabei können Sie zwischen Kilobit (KBit), Megabit (MBit) und Gigabit (GBit) pro Sekunde wählen.

Seien Sie vorsichtig, wenn Sie diese Funktion konfigurieren, da es durch Begrenzen des Datenverkehrs zu Datenverlusten kommen kann.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Netzwerkeinstellungen** und dann auf die Registerkarte **Datenverkehr**.

Die vorhandenen Steuerungen werden in der Tabelle aufgeführt.

3 Zum Hinzufügen von Steuerungen für ein Gerät klicken Sie auf **Hinzufügen**, geben Sie die Netzwerkadresse und die Maske ein, legen Sie die Rate fest, und klicken Sie dann auf **OK**.

Wenn Sie die Maske auf Null (0) festlegen, werden alle gesendeten Daten gesteuert.

4 Klicken Sie auf **Anwenden**.

Die Geschwindigkeit des ausgehenden Datenverkehrs wird für die angegebene Netzwerkadresse gesteuert.

Arbeiten mit Hostnamen

Der Hostname eines Geräts ist meist hilfreicher als die IP-Adresse. Sie können Hostnamen verwalten, um sie der entsprechenden IP-Adresse zuzuordnen.

Auf der Seite **Hosts** können Sie Hostnamen hinzufügen, bearbeiten, entfernen, suchen, aktualisieren und importieren. Außerdem können Sie festlegen, wann ein automatisch erlernter Hostname abläuft.

Beim Anzeigen von Ereignisdaten können Sie die Hostnamen anzeigen, die den IP-Adressen im Ereignis zugeordnet sind. Dazu klicken Sie unten in Ansichtskomponenten auf das Symbol **Hostnamen anzeigen**  . Wenn vorhandene Ereignisse nicht mit einem Hostnamen gekennzeichnet sind, wird die Host-Tabelle auf dem ESM vom System durchsucht, und die IP-Adressen werden mit den zugehörigen Hostnamen gekennzeichnet. Wenn die IP-Adressen nicht in der Host-Tabelle aufgeführt sind, werden die Hostnamen mithilfe einer DNS-Suche (Domain Name System) ausfindig gemacht. Die Suchergebnisse werden dann in der Ansicht angezeigt und zur Host-Tabelle hinzugefügt. In der Host-Tabelle werden die Daten als **Automatisch erlernt** markiert und laufen nach dem Zeitraum ab, den Sie im Feld **Einträge laufen ab nach** unter der Host-Tabelle auf der Seite **Systemeigenschaften** | **Hosts** den Umgehungsmodus für das Gerät zu deaktivieren. Nach Ablauf der Daten wird eine weitere DNS-Suche ausgeführt, sobald Sie wieder in einer Ansicht die Option **Hostnamen anzeigen** auswählen.

In der Host-Tabelle werden automatisch erlernte und hinzugefügte Hostnamen und die zugehörigen IP-Adressen aufgeführt. Sie können manuell Informationen zur Host-Tabelle hinzufügen, indem Sie einen Hostnamen und eine IP-Adresse einzeln eingeben oder eine durch Tabstopps getrennte Liste mit Hostnamen und IP-Adressen importieren. Je mehr Daten Sie auf diese Weise eingeben, umso weniger Zeitaufwand entsteht für DNS-Suchen. Wenn Sie einen Hostnamen manuell eingeben, läuft dieser nicht ab. Sie können ihn jedoch bearbeiten oder entfernen.

Verwalten von Hostnamen

Führen Sie auf der Seite **Hosts** alle erforderlichen Aktionen zum Verwalten der Hostnamen aus, beispielsweise Hinzufügen, Bearbeiten, Importieren, Entfernen oder Suchen. Außerdem können Sie das Ablaufdatum für automatisch erlernte Hosts festlegen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Hosts**.
2. Wählen Sie eine Option aus, und geben Sie die erforderlichen Informationen ein.
3. Klicken Sie auf **Anwenden** oder **OK**.

Einrichten von DHCP

Mithilfe von DHCP (Dynamic Host Configuration Protocol) werden in IP-Netzwerken Konfigurationsparameter wie beispielsweise IP-Adressen für Schnittstellen und Dienste dynamisch verteilt.

Wenn Sie ESM für die Bereitstellung in der Cloud-Umgebung einrichten, wird DHCP automatisch aktiviert, und es wird eine IP-Adresse zugewiesen. Außerhalb der Cloud-Umgebung können Sie DHCP-Dienste in ESM, in Nicht-HA-Empfängern, in ACE und in ELM aktivieren und deaktivieren, wenn Sie über Rechte zur Geräteverwaltung verfügen. Dies ist hilfreich, wenn Sie die IP-Adressen für das Netzwerk zurücksetzen müssen.



Aliasse sind deaktiviert, wenn DHCP aktiviert ist.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System oder ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Führen Sie eine der folgenden Aktionen aus:

- Für ESM: Klicken Sie auf **Netzwerkeinstellungen** und dann auf die Registerkarte **Hauptbildschirm**.
- Für ein Gerät: Wählen Sie die entsprechende Option **Konfiguration** aus, klicken Sie auf **Schnittstellen** und dann auf die Registerkarte **Netzwerk**.

3 Klicken Sie für das Feld **Schnittstelle 1** auf **Setup**, und wählen Sie dann **DHCP** aus.

Wenn es sich bei den Geräten nicht um Empfänger handelt, werden Sie informiert, dass der ESM-Server für die Änderungen neu gestartet werden muss.

4 Klicken Sie auf **OK**.

Einrichten von DHCP in einem VLAN

Mithilfe von DHCP (Dynamic Host Configuration Protocol) werden in IP-Netzwerken Konfigurationsparameter wie beispielsweise IP-Adressen für Schnittstellen und Dienste dynamisch verteilt.

Wenn Sie ESM für die Bereitstellung in der Cloud-Umgebung einrichten, wird DHCP automatisch aktiviert, und es wird eine IP-Adresse zugewiesen. Außerhalb der Cloud-Umgebung können Sie DHCP-Dienste in den VLANs, in ESM, in Nicht-HA-Empfängern, in ACE und in ELM aktivieren und deaktivieren, wenn Sie über Rechte zur Geräteverwaltung verfügen. Dies ist hilfreich, wenn Sie die IP-Adressen für das Netzwerk zurücksetzen müssen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System oder ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Führen Sie eine der folgenden Aktionen aus:

- Für ESM: Klicken Sie auf **Netzwerkeinstellungen** und dann auf die Registerkarte **Hauptbildschirm**.
- Für ein Gerät: Wählen Sie die entsprechende Option **Konfiguration** aus, klicken Sie auf **Schnittstellen** und dann auf die Registerkarte **Netzwerk**.

3 Klicken Sie für das Feld **Schnittstelle 1** auf **Setup**, und klicken Sie dann auf **Erweitert**.

4 Klicken Sie auf **VLAN hinzufügen**, geben Sie das **VLAN** ein, und wählen Sie dann **DHCP** aus.

5 Klicken Sie auf **OK**, um zur Seite **Netzwerkeinstellungen** zurückzukehren, und klicken Sie dann auf **Anwenden**.

Wenn es sich bei den Geräten nicht um Empfänger handelt, werden Sie informiert, dass der ESM-Server für die Änderungen neu gestartet werden muss.

Systemzeitsynchronisierung

Da die von ESM und den zugehörigen Geräten generierten Aktivitäten mit einem Zeitstempel versehen sind, müssen ESM und die Geräte unbedingt synchronisiert werden. Nur so ist gewährleistet, dass der

Bezugsrahmen für alle gesammelten Daten gleich ist. Sie können die ESM-Systemzeit festlegen oder ESM und die Geräte über einen NTP-Server synchronisieren lassen.

Einrichten der Systemzeit

Bevor Sie beginnen

Wenn Sie NTP-Server zum ESM-Gerät hinzufügen möchten, richten Sie die NTP-Server ein, und halten Sie die zugehörigen Autorisierungsschlüssel und Schlüssel-IDs bereit.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und vergewissern Sie sich, dass **Systeminformationen** ausgewählt ist.
2. Klicken Sie auf **Systemuhr (GMT)**, definieren Sie die Einstellungen, und klicken Sie dann auf **OK**.



Bei den NTP-Server-Adressen von Geräten der IPS-Klasse muss es sich um IP-Adressen handeln.

Die Server-Informationen werden in der Konfigurationsdatei gespeichert. Anschließend können Sie wieder die Liste der NTP-Server öffnen und ihren Status überprüfen.

Synchronisieren der Geräteuhren

Sie können die Geräteuhren mit der Uhr des ESM-Geräts synchronisieren, damit die von den verschiedenen System generierten Daten die gleiche Zeiteinstellung widerspiegeln.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** oder die Option **Eigenschaften** für das jeweilige Gerät aus, und klicken Sie dann im Feld **Geräteuhr synchronisieren** auf **Synchronisieren**.

   Wenn die Synchronisierung abgeschlossen ist oder ein Problem aufgetreten ist, werden Sie informiert.
2. Klicken Sie auf **Aktualisieren**, um die Daten auf der Seite **Systeminformationen** oder auf der Seite **Informationen** für das jeweilige Gerät zu aktualisieren.

Installieren eines neuen Zertifikats

Im Lieferumfang des ESM-Geräts ist ein standardmäßiges selbstsigniertes Sicherheitszertifikat für esm.mcafee.local enthalten. In den meisten Web-Browsern wird eine Warnmeldung angezeigt, dass die Authentizität des Zertifikats nicht überprüft werden kann. Wenn Sie das Paar aus SSL-Schlüssel und Zertifikat abgerufen haben, das Sie für das ESM-Gerät verwenden möchten, müssen Sie es installieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **ESM-Verwaltung**.
2. Klicken Sie auf der Registerkarte **Schlüsselverwaltung** auf **Zertifikat**.
3. Wählen Sie die entsprechenden Optionen aus, und klicken Sie dann auf **Schließen**.

Konfigurieren von Profilen

Definieren Sie Profile für Syslog-basierten Datenverkehr, damit Sie Setups mit gemeinsamen Informationen ausführen können, ohne die Details jedes Mal einzugeben. Außerdem können Sie ein Profil für Remote-Befehle (URL oder Skript) hinzufügen und es für eine Ansicht und einen Alarm verwenden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Profilverwaltung**.
2. Zum Hinzufügen eines Profils klicken Sie auf der Registerkarte **Systemprofile** auf **Hinzufügen**, und geben Sie dann die Profildaten ein.
3. Zum Hinzufügen eines Remote-Befehls klicken Sie auf die Registerkarte **Remote-Befehl**, und geben Sie dann die erforderlichen Informationen ein.
4. Klicken Sie auf **OK**.

SNMP-Konfiguration

Konfigurieren Sie die Einstellungen, die vom ESM-Gerät zum Senden von Traps für Verbindung aktiv, Verbindung inaktiv, Kaltstart und Warmstart (vom ESM-Gerät sowie von den einzelnen Geräten) verwendet werden. Rufen Sie System- und Schnittstellentabellen für Management Information Base (MIB) II ab, und lassen Sie die Erkennung des ESM-Geräts mit dem snmpwalk-Befehl zu.

SNMPv3 wird mit den Optionen NoAuthNoPriv, AuthNoPriv und AuthPriv unterstützt. Dabei wird MD5 oder SHA (Secure Hash Algorithm) für die Authentifizierung und DES (Data Encryption Standard) oder AES (Advanced Encryption Standard) für die Verschlüsselung verwendet (MD5 und DES sind im FIPS-Compliance-Modus nicht verfügbar).

SNMP-Anfragen können an ein ESM-System gesendet werden, um Integritätsinformationen für ESM, einen Empfänger und Nitro IPS abzurufen. SNMPv3-Traps können an ein ESM-Gerät gesendet werden, um sie zur Blacklist mindestens eines der verwalteten Nitro IPS-Geräte hinzuzufügen. Alle McAfee-Appliances können außerdem für das Senden von Traps für Verbindung aktiv, Verbindung inaktiv, Kaltstart und Warmstart an mindestens ein Ziel Ihrer Wahl konfiguriert werden (siehe *SNMP und McAfee-MIB*).

Konfigurieren von SNMP-Einstellungen

Definieren Sie die Einstellungen, die vom ESM-Gerät für eingehenden und ausgehenden SNMP-Datenverkehr verwendet werden. SNMP-Abfragen können nur von Benutzern ausgeführt werden, deren Benutzernamen kein Leerzeichen enthalten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **SNMP-Konfiguration**.
2. Geben Sie auf den Registerkarten **SNMP-Anfragen** und **SNMP-Traps** die erforderlichen Informationen ein.
3. Klicken Sie auf **OK**.

Einrichten von SNMP-Traps zur Benachrichtigung bei Stromausfällen

Wählen Sie einen SNMP-Trap aus, durch den Sie über allgemeine Hardware-Fehler und Ausfälle der Stromversorgung von DAS-Geräten benachrichtigt werden, damit Sie das Herunterfahren von Geräten bei Stromausfällen vermeiden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **SNMP-Konfiguration**, klicken Sie auf die Registerkarte **SNMP-Traps**, und wählen Sie dann **Allgemeiner Hardware-Fehler** aus.
3. Klicken Sie auf **Anwenden** oder **OK**.

Beim Ausfall einer Stromversorgung wird ein SNMP-Trap gesendet, und in der Systemnavigationsstruktur wird neben dem Gerät eine Kennzeichnung für den Integritätsstatus angezeigt.

Sie können einen Alarm hinzufügen, der bei Auftreten eines Fehlers ausgelöst wird (siehe *Hinzufügen eines Alarms zur Benachrichtigung bei Stromausfällen*).

Erstellen eines SNMP-Traps als Aktion in einem Alarm

Sie können SNMP-Traps als Aktion innerhalb eines Alarms senden.

Bevor Sie beginnen

Bereiten Sie den SNMP-Trap-Empfänger vor (nur erforderlich, wenn kein SNMP-Trap-Empfänger vorhanden ist).

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1. Erstellen Sie ein SNMP-Profil, um für ESM anzugeben, wohin die SNMP-Traps gesendet werden sollen.
   a. Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
   b. Klicken Sie auf **Profilverwaltung**, und wählen Sie dann im Feld **Profiltyp** die Option **SNMP-Trap** aus.
   c. Füllen Sie die verbleibenden Felder aus, und klicken Sie dann auf **Anwenden**.

2 Konfigurieren Sie SNMP in ESM.

   a Klicken Sie in **Systemeigenschaften** auf **SNMP-Konfiguration** und dann auf die Registerkarte **SNMP-Traps**.

   b Wählen Sie den Port aus, wählen Sie die Trap-Typen aus, die gesendet werden sollen, und wählen Sie dann das in Schritt 1 hinzugefügte Profil aus.

   c Klicken Sie auf **Anwenden**.

3 Definieren Sie einen Alarm mit der Aktion **SNMP-Trap**.

   a Klicken Sie in **Systemeigenschaften** auf **Alarme** und dann auf **Hinzufügen**.

   b Geben Sie auf den Registerkarten **Zusammenfassung**, **Bedingung** und **Geräte** die erforderlichen Informationen ein. Wählen Sie den Bedingungstyp **Interne Ereignisübereinstimmung** aus, und klicken Sie dann auf die Registerkarte **Aktionen**.

   c Wählen Sie **Nachricht senden** aus, und klicken Sie dann auf **Konfigurieren**, um eine Vorlage für SNMP-Nachrichten auszuwählen oder zu erstellen.

   d Wählen Sie im Feld **SNMP** die Option **Standard-SNMP-Trap** aus, oder klicken Sie auf **Vorlagen** und dann auf **Hinzufügen**.

   e Wählen Sie eine vorhandene Vorlage aus, oder klicken Sie auf **Hinzufügen**, um eine neue Vorlage zu definieren.

   f Kehren Sie zur Seite **Alarmeinstellungen** zurück, und fahren Sie mit dem Einrichten des Alarms fort.

Hinzufügen eines Alarms zur Benachrichtigung bei Stromausfällen

Fügen Sie einen Alarm hinzu, damit Sie bei Ausfall einer der ESM-Stromversorgungen benachrichtigt werden.

> **Bevor Sie beginnen**
>
> Richten Sie einen SNMP-Trap für allgemeine Hardware-Fehler ein (siehe *Einrichten eines SNMP-Traps für Benachrichtigung bei Stromausfällen*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Alarme**, klicken Sie auf **Hinzufügen**, fügen Sie auf der Registerkarte **Übersicht** die erforderlichen Daten hinzu, und klicken Sie dann auf die Registerkarte **Bedingung**.

3 Wählen Sie im Feld **Typ** die Option **Interne Ereignisübereinstimmung** aus.

4 Wählen Sie im Feld **Feld** die Option **Signatur-ID** aus, und geben Sie dann `306-50086` in das Feld **Werte** ein.

5 Füllen Sie nach Bedarf die verbleibenden Informationen auf den einzelnen Registerkarten aus, und klicken Sie dann auf **Fertig stellen**.

Bei Ausfall einer Stromversorgung wird ein Alarm ausgelöst.

SNMP und McAfee-MIB

Auf verschiedene Aspekte der McAfee-Produktlinie können Sie über SNMP zugreifen. In der McAfee-MIB werden die Objekt-IDs (OIDs) für die einzelnen relevanten Objekte oder Merkmale definiert.

In der MIB werden Objektgruppen für Folgendes definiert:

- **Warnungen**: Auf einem ESM-Gerät können Warnungs-Traps mithilfe der Ereignisweiterleitung generiert und gesendet werden. Sie können auf einem Empfänger Warnungs-Traps empfangen, indem Sie eine McAfee-SNMP-Datenquelle konfigurieren.
- **Flüsse**: Sie können auf einem Empfänger Fluss-Traps empfangen, indem Sie eine McAfee-SNMP-Datenquelle konfigurieren.
- **ESM-Integritätsanfragen**: Auf einem ESM-Gerät können Integritätsanfragen für das Gerät selbst sowie für die über das Gerät verwalteten Geräte empfangen und beantwortet werden.
- **Blacklist**: Auf einem ESM-Geräte können Traps empfangen werden, mit denen Einträge für Blacklists und Quarantänelisten definiert werden, die dann auf die von diesem Gerät verwalteten Nitro IPS-Geräte angewendet werden.

Außerdem werden in der McAfee-MIB Textkonventionen (aufgezählte Typen) für Werte definiert. Dazu gehören:

- Die bei Empfang einer Warnung ausgeführte Aktion
- Richtung und Status von Flüssen
- Datenquellentypen
- Blacklist-Aktionen

Die Syntax der McAfee-MIB ist SMI-konform (SNMPv2 Structure of Management Information). McAfee-Produkte, in denen SNMP verwendet wird, können für den Betrieb über SNMPv1, SNMPv2c und SNMPv3 konfiguriert werden (einschließlich Authentifizierung und Zugriffssteuerung).

Für Integritätsanfragen wird der SNMP `GET`-Vorgang verwendet. Der SNMP `GET`-Vorgang wird von SNMP-Manager-Anwendungen verwendet, um Werte von den Objekten abzurufen, die vom SNMP-Agenten (in diesem Fall ESM-Gerät) verwaltet werden. Von den Anwendung wird in der Regel eine SNMP GET-Anfrage ausgeführt. Dabei werden der Hostname des ESM-Geräts und OIDs sowie die konkrete Instanz der OID angegeben.

Das ESM-Gerät antwortet mit einem Rückgabewert oder einem Fehler. Beispiel: Eine Integritätsanfrage und die entsprechende Antwort für die Integrität des Nitro IPS-Geräts mit der Nitro IPS-ID 2 könnte so aussehen:

Anfrage- und Antwort-OID	Einheiten	Antwortwert	Bedeutung
1.3.6.1.4.1.23128.1.3.2.1.2		Intern	Name des Nitro IPS-Geräts
1.3.6.1.4.1.23128.1.3.2.2.2		2	Eindeutige ESM-ID des Nitro IPS-Geräts
1.3.6.1.4.1.23128.1.3.2.3.2		1	Weist darauf hin, dass die Kommunikation mit dem Nitro IPS-Gerät verfügbar (1) oder nicht verfügbar (0) ist."
1.3.6.1.4.1.23128.1.3.2.4.2		OK	Status des Nitro IPS-Geräts
1.3.6.1.4.1.23128.1.3.2.5.2		aus	Status der Umgehungs-Netzwerkkarten des Nitro IPS-Geräts

Anfrage- und Antwort-OID	Einheiten	Antwortwert	Bedeutung
1.3.6.1.4.1.23128.1.3.2.6.2		Nitro IPS	Modus des Nitro IPS-Geräts (Nitro IPS oder IDS)
1.3.6.1.4.1.23128.1.3.2.7.2	Prozent	2	Prozentsatz für die kombinierte unmittelbare CPU-Auslastung
1.3.6.1.4.1.23128.1.3.2.8.2	MB	1010	RAM des Nitro IPS-Geräts insgesamt
1.3.6.1.4.1.23128.1.3.2.9.2	MB	62	Verfügbares RAM
1.3.6.1.4.1.23128.1.3.2.10.2	MB	27648	Gesamter partitionierter Festplatten-Speicherplatz für die Nitro IPS-Datenbank
1.3.6.1.4.1.23128.1.3.2.11.2	MB	17408	Freier verfügbarer Festplatten-Speicherplatz für die Nitro IPS-Datenbank
1.3.6.1.4.1.23128.1.3.2.12.2	Sekunden seit dem 01.01.1970 00:00:00.0 (GMT)	120793661	Aktuelle Systemzeit des Nitro IPS-Geräts
1.3.6.1.4.1.23128.1.3.2.13.2		7.1.3 20070518091421a	Versionsinformationen und Build-Stempel des Nitro IPS-Geräts
1.3.6.1.4.1.23128.1.3.2.14.2		ABCD:1234	Computer-ID des Nitro IPS-Geräts
1.3.6.1.4.1.23128.1.3.2.15.2		Nitro IPS	Modellnummer des Nitro IPS-Geräts
1.3.6.1.4.1.23128.1.3.2.16.2	Warnungen pro Minute	140	Warnungsrate (pro Minute) für mindestens zehn Minuten
1.3.6.1.4.1.23128.1.3.2.17.2	Flüsse pro Minute	165	Flussrate (pro Minute) für mindestens zehn Minuten

Im oben genannten Beispiel wird vom SNMP-Manager eine Anfrage an den SNMP-Agenten (das ESM-Gerät) gesendet. Die Zahlen haben folgende Bedeutung:

- 1.3.6.1.4.1.23128 ist die Unternehmensnummer, die McAfee von der IANA (Internet Assigned Numbers Authority) zugewiesen wurde.
- 1.3.2 ist eine Nitro IPS-Integritätsanfrage.
- Die vorletzte Zahl (oben 1 – 17) wird zum Anfragen der verschiedenen Aspekte der Nitro IPS-Integrität verwendet.
- Die letzte Zahl (2) gibt die konkrete Instanz der OID an, die Nitro IPS-ID.

Als Antwort vom ESM-Gerät werden die OID-Bindungen mit den Ergebnissen der Integritätsanfrage ausgefüllt.

In den folgenden Tabellen finden Sie die Bedeutung der ESM- und Empfänger-OIDs.

Tabelle 3-37 ESM-Integrität

Anfrage- und Antwort-OID	Einheiten	Antwortwert	Bedeutung
1.3.6.1.4.1.23128.1.3.1.1	Prozent	4	Prozentsatz für die kombinierte unmittelbare CPU-Auslastung
1.3.6.1.4.1.23128.1.3.1.2	MB	3518	RAM insgesamt
1.3.6.1.4.1.23128.1.3.1.3	MB	25	Verfügbares RAM
1.3.6.1.4.1.23128.1.3.1.4	MB	1468006	Gesamter partitionierter Festplatten-Speicherplatz für die ESM-Datenbank
1.3.6.1.4.1.23128.1.3.1.5	MB	1363148	Freier verfügbarer Festplatten-Speicherplatz für die ESM-Datenbank
1.3.6.1.4.1.23128.1.3.1.6	Sekunden seit dem 01.01.1970 00:00:0.0 (GMT)	1283888714	Aktuelle Systemzeit des ESM-Geräts
1.3.6.1.4.1.23128.1.3.1.7		8.4.2	Version und Build-Stempel von ESM
1.3.6.1.4.1.23128.1.3.1.8		4EEE:6669	Computer-ID des ESM-Geräts
1.3.6.1.4.1.23128.1.3.1.9		ESM	Modellnummer des ESM-Geräts

Tabelle 3-38 Integrität des Empfängers

Anfrage- und Antwort-OID	Einheiten	Antwortwert	Bedeutung
1.3.6.1.4.1.23128.1.3.3.1		Empfänger	Name des Empfängers
1.3.6.1.4.1.23128.1.3.3.2		2689599744	Eindeutige ESM-ID des Empfängers
1.3.6.1.4.1.23128.1.3.3.3		1	Weist darauf hin, dass die Kommunikation mit dem Empfänger verfügbar (1) oder nicht verfügbar (0) ist.
1.3.6.1.4.1.23128.1.3.3.4		OK	Gibt den Status des Empfängers an.
1.3.6.1.4.1.23128.1.3.3.5	Prozent	2	Prozentsatz für die kombinierte unmittelbare CPU-Auslastung
1.3.6.1.4.1.23128.1.3.3.6	MB	7155	RAM insgesamt
1.3.6.1.4.1.23128.1.3.3.7	MB	5619	Verfügbares RAM
1.3.6.1.4.1.23128.1.3.3.8	MB	498688	Gesamter partitionierter Festplatten-Speicherplatz für die Empfängerdatenbank
1.3.6.1.4.1.23128.1.3.3.9	MB	472064	Freier verfügbarer Festplatten-Speicherplatz für die Empfängerdatenbank

Tabelle 3-38 Integrität des Empfängers *(Fortsetzung)*

Anfrage- und Antwort-OID	Einheiten	Antwortwert	Bedeutung
1.3.6.1.4.1.23128.1.3.3.10	Sekunden seit dem 01.01.1970 00:00:0.0 (GMT)	1283889234	Aktuelle Systemzeit des Empfängers
1.3.6.1.4.1.23128.1.3.3.11		7.1.3 20070518091421a	Version und Build-Stempel des Empfängers
1.3.6.1.4.1.23128.1.3.3.12		5EEE:CCC6	Computer-ID des Empfängers
1.3.6.1.4.1.23128.1.3.3.13		Empfänger	Modellnummer des Empfängers
1.3.6.1.4.1.23128.1.3.3.14	Warnungen pro Minute	1	Warnungsrate (pro Minute) für mindestens zehn Minuten
1.3.6.1.4.1.23128.1.3.3.15	Flüsse pro Minute	2	Flussrate (pro Minute) für mindestens zehn Minuten

Ereignisse, Flüsse und Blacklist-Einträge werden mit SNMP-Traps oder Informationsanfragen gesendet. Ein Warnungs-Trap, der von einem für die Ereignisweiterleitung konfigurierten ESM-Gerät gesendet wird, kann in etwa so aussehen:

OID	Wert	Bedeutung
1.3.6.1.4.1.23128.1.1.1	780	ESM-Warnungs-ID
1.3.6.1.4.1.23128.1.1.2	6136598	Warnungs-ID des Geräts
1.3.6.1.4.1.23128.1.1.3	Intern	Gerätename
1.3.6.1.4.1.23128.1.1.4	2	Geräte-ID
1.3.6.1.4.1.23128.1.1.5	10.0.0.69	Quell-IP
1.3.6.1.4.1.23128.1.1.6	27078	Quell-Port
1.3.6.1.4.1.23128.1.1.7	AB:CD:EF:01:23:45	Quell-MAC
1.3.6.1.4.1.23128.1.1.8	10.0.0.68	Ziel-IP
1.3.6.1.4.1.23128.1.1.9	37258	Ziel-Port
1.3.6.1.4.1.23128.1.1.10	01:23:45:AB:CD:EF	Ziel-MAC
1.3.6.1.4.1.23128.1.1.11	17	Protokoll
1.3.6.1.4.1.23128.1.1.12	0	VLAN
1.3.6.1.4.1.23128.1.1.13	1 Richtung	
1.3.6.1.4.1.23128.1.1.14	20	Ereignisanzahl
1.3.6.1.4.1.23128.1.1.15	1201791100	Erstes Mal
1.3.6.1.4.1.23128.1.1.16	1201794638	Letztes Mal
1.3.6.1.4.1.23128.1.1.17	288448	Letztes Mal (Mikrosekunden)
1.3.6.1.4.1.23128.1.1.18	2000002	Signatur-ID

OID	Wert	Bedeutung
1.3.6.1.4.1.23128.1.1.19	ANOMALY Inbound High to High	Signaturbeschreibung
1.3.6.1.4.1.23128.1.1.20	5	Ausgeführte Aktion
1.3.6.1.4.1.23128.1.1.21	1	Schweregrad
1.3.6.1.4.1.23128.1.1.22	201	Datenquellentyp oder Ergebnis
1.3.6.1.4.1.23128.1.1.23	0	Normalisierte Signatur-ID
1.3.6.1.4.1.23128.1.1.24	0:0:0:0:0:0:0:0	IPv6-Quell-IP
1.3.6.1.4.1.23128.1.1.25	0:0:0:0:0:0:0:0	IPv6-Ziel-IP
1.3.6.1.4.1.23128.1.1.26		Application
1.3.6.1.4.1.23128.1.1.27		Domäne
1.3.6.1.4.1.23128.1.1.28		Host
1.3.6.1.4.1.23128.1.1.29		Benutzer (Quelle)
1.3.6.1.4.1.23128.1.1.30		Benutzer (Ziel)
1.3.6.1.4.1.23128.1.1.31		Befehl
1.3.6.1.4.1.23128.1.1.32		Objekt
1.3.6.1.4.1.23128.1.1.33		Sequenznummer
1.3.6.1.4.1.23128.1.1.34		Gibt an, ob das Ereignis in einer vertrauenswürdigen oder nicht vertrauenswürdigen Umgebung generiert wurde.
1.3.6.1.4.1.23128.1.1.35		Die ID der Sitzung, in der die Warnung generiert wurde.

Die Zahlen haben folgende Bedeutung:

- 1.3.6.1.4.1.23128 ist die Unternehmensnummer, die McAfee von der IANA zugewiesen wurde.
- 1.1 ist eine Nitro IPS-Integritätsanfrage.
- Die letzte Zahl (1 – 35) wird für die Berichterstellung im Zusammenhang mit den verschiedenen Merkmalen der Warnung verwendet.

Sämtliche Details der McAfee-MIB-Definition finden Sie unter https://x.x.x.x/BrowseReference/NITROSECURITY-BASE-MIB.txt, wobei x.x.x.x der IP-Adresse Ihres ESM-Geräts entspricht.

Verwalten der Datenbank

Verwalten Sie die ESM-Datenbank, um Informationen und Einstellungen anzugeben, während Sie die Funktionen im System einrichten.

Sie können Indexeinstellungen für die Datenbank verwalten, Informationen zur Speicherverwendung der Datenbank durch Ereignisse und Flüsse anzeigen und drucken, Speicherorte für inaktive Partitionen, die Datenbeibehaltungs-Richtlinie für Ereignisse und Flüsse sowie die Speicherplatzzuordnung für Ereignis- und Flussdaten in der Datenbank konfigurieren.

Bei einer VM mit mehr als vier CPUs können Sie den zusätzlichen Speicherplatz als Systemspeicher, Datenspeicher und Hochleistungsspeicher verwenden.

Wenn Sie mehrere Laufwerke gleichzeitig aus der ESM-VM entfernen, gehen möglicherweise alle vorherigen ELM-Suchen verloren. Dies können Sie verhindern, indem Sie die ELM-Suchergebnisse exportieren, bevor Sie diesen Vorgang ausführen.

Siehe auch

Verwalten der Akkumulator-Indizierung auf Seite 198
Verwalten von Indexeinstellungen für die Datenbank auf Seite 198
Einrichten von Datenbeibehaltungs-Limits auf Seite 197
Anzeigen der Speicherverwendung der Datenbank auf Seite 199

Einrichten des ESM-Datenspeichers

Zum Speichern von ESM-Daten können Sie drei externe Speichertypen einrichten: Internet Small Computer System Interface (iSCSI), Storage Area Network (SAN) und Direct-Attached Storage (DAS). Wenn diese Speichertypen mit dem ESM-Gerät verbunden sind, können Sie sie für die Speicherung von Daten vom ESM-Gerät einrichten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Database** | **Datenspeicher**.
2. Klicken Sie auf eine der Registerkarten, wählen Sie eine Aktion aus, und geben Sie dann die erforderlichen Informationen ein.
3. Klicken Sie auf **Abbrechen**, um die Seite zu schließen.

Siehe auch

Einrichten von Datenbeibehaltungs-Limits auf Seite 197

Einrichten des ESM-VM-Datenspeichers

Wenn die ESM-VM mehr als vier CPUs hat, steht auf der Seite **Datenbank** die Option **VM-Daten** zur Verfügung. Mit dieser Option können Sie den zusätzlichen Speicher verwenden, der für den Systemspeicher, Datenspeicher und Hochleistungsspeicher der VM verfügbar ist.

Jede Dropdown-Liste auf der Seite **Datenzuordnung** enthält die verfügbaren Speicherlaufwerke, die in der VM bereitgestellt sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Database** | **VM-Daten**.
2. Wählen Sie in jedem Feld das Laufwerk aus, auf dem die Daten gespeichert werden sollen. Jedes Laufwerk kann nur einmal ausgewählt werden.
3. Klicken Sie auf **OK**.

Erhöhen der Anzahl verfügbarer Akkumulator-Indizes

Aufgrund der Anzahl der aktivierten Standard-Indizes auf dem ESM-Gerät können Sie nur fünf Indizes zu einem Akkumulator-Feld hinzufügen. Wenn Sie mehr als fünf benötigen, können Sie zurzeit nicht

verwendete Standard-Indizes deaktivieren, beispielsweise sessionid, src/dst mac, src/dst port, src/dst zone oder src/dst geolocation (maximal 42).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.



In ESM werden beim Generieren von Abfragen, Berichten, Alarmen und Ansichten Standard-Indizes verwendet. Falls Sie Standard-Indizes deaktivieren und Abfragen, Berichte, Alarme oder Ansichten zu generieren versuchen, die diese Standard-Indizes verwenden, werden Sie informiert, dass sie aufgrund eines deaktivierten Indexes nicht verarbeitet werden können. Sie erfahren nicht, welcher Index den Vorgang beeinträchtigt. Aufgrund dieser Einschränkung sollten Sie Standard-Indizes nur deaktivieren, wenn dies wirklich erforderlich ist.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Datenbank**.
2. Klicken Sie auf **Einstellungen** und dann auf die Registerkarte **Akkumulator-Indizierung**.
3. Klicken Sie in der Dropdown-Liste auf **Standard-Indizes**, und wählen Sie dann **Standard-Indizes anzeigen** aus.

   Die Standard-Indizes werden im Bereich **Aktiviert** aufgeführt.
4. Klicken Sie auf die Standard-Indizes, die deaktiviert werden sollen, und klicken Sie dann auf den Pfeil, um sie in den Bereich **Verfügbar** zu verschieben.

   Die Zahl in der Angabe **verbleibend** in der rechten oberen Ecke der Seite wird mit jedem deaktivierten Standard-Index erhöht.

Jetzt können Sie mehr als fünf Akkumulator-Indizes für das ausgewählte Akkumulator-Feld aktivieren (siehe *Verwalten der Akkumulator-Indizierung*).

Einrichten des Archivs für inaktive Partitionen

Die Daten von ESM sind in Partitionen unterteilt. Wenn die maximale Größe einer Partition erreicht ist, wird die Partition inaktiv und wird gelöscht. Sie können einen Speicherort für inaktive Partitionen konfigurieren, damit diese nicht gelöscht werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Database** | **Archivierung**.
2. Füllen Sie die Felder aus, die vom ausgewählten Typ abhängen.
3. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Inaktive Partitionen werden an diesen Speicherort kopiert und auf den Registerkarten **Ereignispartitionen** und **Flusspartitionen** aufgeführt.

Einrichten von Datenbeibehaltungs-Limits

Wenn Sie eine Konfiguration haben, bei der historische Daten an das System gesendet werden, können Sie auswählen, wie lange Ereignisse und Flüsse beibehalten werden sollen und wie viele historische Daten maximal eingefügt werden sollen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Database** | **Datenbeibehaltung**.
2. Wählen Sie aus, wie lange Ereignisse und Flüsse beibehalten werden sollen und ob Sie historische Daten einschränken möchten.
3. Klicken Sie auf **OK**.

Siehe auch

Einrichten des ESM-Datenspeichers auf Seite 196

Definieren von Datenzuordnungslimits

Die maximale Anzahl der vom System verwalteten Ereignis- und Flussdatensätze ist ein fester Wert. Mithilfe der Datenzuordnung können Sie festlegen, wie viel Speicherplatz jeweils zugeordnet werden soll, und wie viele Datensätze durchsucht werden, um Abfragen zu optimieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Database** | **Datenzuordnung**.
2. Klicken Sie auf die Markierungen der Zahlenzeilen und ziehen Sie sie auf die gewünschten Zahlen. Alternativ können Sie auf die Pfeile in den Feldern **Ereignisse** und **Flüsse** klicken.
3. Klicken Sie auf **OK**.

Verwalten von Indexeinstellungen für die Datenbank

Konfigurieren Sie Optionen für die Indizierung bestimmter Datenfelder in der Datenbank. Nicht indizierte Daten werden zwar gespeichert, aber in den meisten Abfrageergebnissen nicht angezeigt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Database** | **Einstellungen**.
2. Zum Ändern der aktuellen Einstellungen in den Spalten **Ereignisse** und **Flüsse** klicken Sie auf das zu ändernde Element, und wählen Sie in der Dropdown-Liste eine neue Einstellung aus.
3. Wenn Sie in den Spalten mit der Bezeichnung **Port** die Option **Benutzerdefiniert** auswählen, wird der Bildschirm **Port-Werte** geöffnet. Hier können Sie einen neuen Port-Wert auswählen oder hinzufügen.
4. Klicken Sie auf **OK**.

Verwalten der Akkumulator-Indizierung

Wenn Sie benutzerdefinierte Felder haben, mit denen numerische Daten aus einer Quelle abgerufen werden, können Sie mit der Akkumulator-Indizierung Durchschnitte im Zeitverlauf für diese Daten

ermitteln. Sie können mehrere Ereignisse akkumulieren und den Durchschnitt ihrer Werte ermitteln oder einen Trendwert generieren.

> **Bevor Sie beginnen**
> Richten Sie einen benutzerdefinierten Typ für die Akkumulator-Indizierung ein (siehe *Erstellen benutzerdefinierter Typen*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Datenbank**.
2. Klicken Sie auf **Einstellungen** und dann auf die Registerkarte **Akkumulator-Indizierung**.
3. Wählen Sie die Indizes aus, und klicken Sie dann auf **OK**.

Nun können Sie eine Akkumulator-Abfrage einrichten, um die Ergebnisse anzuzeigen.

Siehe auch

Verwalten von Abfragen auf Seite 290
Erstellen benutzerdefinierter Typen auf Seite 305

Anzeigen der Speicherverwendung der Datenbank

Sie können Tabellen anzeigen und drucken, aus denen hervorgeht, wie der Datenbankspeicher verwendet wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Database | Speicherverwendung**.

   In den Tabellen **Ereignisse** und **Flüsse** wird die Speicherverwendung der Datenbank aufgeführt.

2. Zum Drucken der Berichte klicken Sie auf das Symbol **Drucken**  .

Arbeiten mit Benutzern und Gruppen

Benutzer und Gruppen müssen zum System hinzugefügt werden, damit sie auf das ESM-Gerät, seine Geräte und Richtlinien sowie die zugeordneten Berechtigungen zugreifen können.

Im FIPS-Modus verfügt ESM über vier mögliche Benutzerrollen: **Benutzer**, **Power-User**, **Administrator für Schlüssel und Zertifikate** und **Audit-Administrator**. Wenn das Gerät nicht im FIPS-Modus betrieben wird, sind zwei Arten von Benutzerkonten möglich: **Systemadministrator** und **allgemeiner Benutzer**.

Die Seite **Benutzer und Gruppen** enthält zwei Abschnitte:

- **Benutzer**: Enthält Namen von Benutzern, die Anzahl der zurzeit geöffneten Sitzungen der einzelnen Benutzer und die Gruppen, denen die Benutzer angehören.
- **Gruppen**: Enthält Namen von Gruppen und eine Beschreibung der Berechtigungen, die den einzelnen Gruppen zugewiesen sind.



Sie können die Tabellen sortieren, indem Sie auf **Benutzername**, **Sitzungen** oder **Gruppenname** klicken.

Gruppenberechtigungen

Beim Einrichten einer Gruppe legen Sie die Berechtigungen für die Mitglieder der Gruppe fest. Wenn Sie unter **Gruppe hinzufügen** auf der Seite **Berechtigungen** die Option **Zugriff dieser Gruppe einschränken** auswählen (**Systemeigenschaften** | **Gruppe hinzufügen**), wird der Zugriff auf diese Funktionen eingeschränkt.

- **Alarme**: Die Benutzer in der Gruppe haben keinen Zugriff auf Empfänger, Dateien oder Vorlagen für die Alarmverwaltung. Sie können keine Alarme erstellen, bearbeiten, entfernen, aktivieren oder deaktivieren.
- **Fallverwaltung**: Kann auf alle Funktionen mit Ausnahme von **Unternehmen** zugreifen.
- **ELM**: Die Benutzer können erweiterte ELM-Suchen ausführen, können aber keine ELM-Suchen speichern und nicht auf Eigenschaften von ELM-Geräten zugreifen.
- **Berichte**: Die Benutzer können nur einen Bericht ausführen, bei dem die Ausgabe per E-Mail gesendet wird.
- **Watchlists**: Die Benutzer können keine dynamische Watchlist hinzufügen.
- **Asset-Manager** und **Richtlinien-Editor**: Die Benutzer können nicht auf diese Funktionen zugreifen.
- **Zonen**: Die Benutzer können nur Zonen anzeigen, auf die sie gemäß ihrer Zonenliste Zugriff haben.
- **Systemeigenschaften**: Kann nur auf **Berichte** und **Überwachungslisten** zugreifen.
- **Filter**: Die Benutzer können nicht auf die Filterregisterkarten **Zeichenfolgennormalisierung**, **Active Directory**, **Ressourcen**, **Ressourcengruppen** oder **Tags** zugreifen.
- Aktionssymbolleiste: Die Benutzer können nicht auf die Geräteverwaltung, die Verwaltung mehrerer Geräte oder die Streaming-Anzeige für Ereignisse zugreifen.

Hinzufügen eines Benutzers

Wenn Sie über Berechtigungen als Systemadministrator verfügen, können Sie Benutzer zum System hinzufügen, damit diese auf das ESM-Gerät, seine Geräte, Richtlinien und zugeordneten Berechtigungen zugreifen können. Hinzugefügte Benutzereinstellungen können bearbeitet oder entfernt werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur Folgendes aus: **Systemeigenschaften** | **Benutzer und Gruppen**.
2. Geben Sie das Kennwort des Systemadministrators ein, und klicken Sie dann auf **OK**.
3. Klicken Sie im Abschnitt **Benutzer** auf **Hinzufügen**, und geben Sie dann die erforderlichen Informationen ein.
4. Klicken Sie auf **OK**.

Benutzer werden mit den Berechtigungen zum System hinzugefügt, die den Gruppen zugewiesen sind, denen sie angehören. Benutzernamen werden auf der Seite **Benutzer und Gruppen** im Abschnitt **Benutzer** angezeigt. Neben jedem Benutzernamen wird ein Symbol angezeigt, aus dem hervorgeht, ob das Konto aktiviert ist. Wenn der Benutzer über Administratorberechtigungen verfügt, wird neben dem Namen ein Symbol mit einem König  angezeigt.

Auswählen von Benutzereinstellungen

Auf der Seite **Benutzereinstellungen** können Sie verschiedene Standardeinstellungen ändern. Sie können die Zeitzone, das Datumsformat, das Kennwort, die Standardanzeige und die Sprache der Konsole

ändern. Außerdem können Sie auswählen, ob deaktivierte Datenquellen und die Registerkarten **Alarme** und **Fälle** angezeigt werden sollen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf der Systemnavigationsleiste der ESM-Konsole auf **Optionen**.

2 Vergewissern Sie sich, dass **Benutzereinstellungen** ausgewählt ist.

3 Nehmen Sie nach Bedarf Änderungen an den Einstellungen vor, und klicken Sie dann auf **OK**.

Die Darstellung der Konsole wird basierend auf den Einstellungen geändert.

Einrichten der Sicherheit

Verwenden Sie die Anmeldesicherheit, um Standardanmeldeeinstellungen einzurichten, die Zugriffssteuerungsliste (ACL, Access Control List) zu konfigurieren und CAC-Einstellungen (Common Access Card) zu definieren. Außerdem können Sie die Authentifizierung über RADIUS (Remote Authentication Dial In User Service), Active Directory und LDAP (Lightweight Directory Access Protocol) aktivieren (nur verfügbar, wenn Sie über die Berechtigungen eines Systemadministrators verfügen).

Sicherheitsfunktionen von ESM

Die Produktfamilie der Nitro IPS-Lösungen von McAfee soll das Auffinden von Netzwerken und vor allem Angriffe erschweren. Da Nitro IPS-Geräte standardmäßig keinen IP-Stack haben, können Pakete nicht direkt an diese Geräte adressiert werden.

Für die Kommunikation mit Nitro IPS-Geräten wird die SEM-Technologie (Secure Encrypted Management) von McAfee verwendet. SEM ist ein mit AES (Advanced Encryption Standard) verschlüsselter In Band-Kanal, durch den das Risiko von Playback- oder Man-in-the-Middle-Angriffen gemindert wird.



Die Kommunikation mit einem Nitro IPS-Gerät ist nur möglich, wenn das Gerät von einem autorisierten ESM-Gerät über den SEM-Kanal adressiert wird. Vom Gerät selbst wird keine Kommunikation initiiert. Die Kommunikation zwischen einem ESM-Gerät und der ESM-Konsole wird ebenfalls mithilfe von AES gesendet.

Auf dem ESM-Gerät werden über einen verschlüsselten Kommunikationsmechanismus authentifizierte und verschlüsselte Signatur- und Software-Aktualisierungen vom zentralen McAfee-Server abgerufen. Durch Hardware- und Software-basierte Mechanismen wird sichergestellt, dass die Geräte nur über ein ordnungsgemäß autorisiertes ESM-Gerät verwaltet werden.

Definieren von Standardanmeldeeinstellungen

Passen Sie die Einstellungen für die Standardanmeldeverfahren an, indem Sie festlegen, wie viele Anmeldeversuche in einem bestimmten Zeitraum möglich sind, wie lange das System inaktiv sein kann, wie die Kennworteinstellungen lauten und ob bei der Anmeldung die letzte Benutzer-ID angezeigt werden soll.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Anmeldesicherheit**.
2. Legen Sie die Optionen auf der Registerkarte **Standard** fest.
3. Klicken Sie auf **OK** oder auf **Anwenden**.

Definieren der Einstellungen für das Anmeldekennwort

Sie können für das Systemanmeldekennwort verschiedene Einstellungen definieren.

> **Bevor Sie beginnen**
> Sie müssen über Systemadministratorrechte verfügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option Systemeigenschaften aus, und klicken Sie dann auf Anmeldesicherheit.
2. Klicken Sie auf die Registerkarte **Kennwörter**, nehmen Sie eine Auswahl vor, und klicken Sie dann auf **Anwenden** oder **OK**.

Konfigurieren von Einstellungen für die RADIUS-Authentifizierung

Konfigurieren Sie das ESM-Gerät für die Authentifizierung von Benutzern gegenüber einem RADIUS-Server.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Anmeldesicherheit**.
2. Wählen Sie die Registerkarte **RADIUS** aus, und füllen Sie dann die Felder für den primären Server aus. Ein sekundärer Server ist optional.
3. Klicken Sie auf **OK** oder auf **Anwenden**.

Wenn der Server aktiviert ist, werden alle Benutzer mit Ausnahme des Systemadministrators über den RADIUS-Server authentifiziert. Wenn die Authentifizierung deaktiviert ist, können Benutzer, die für die RADIUS-Authentifizierung eingerichtet sind, nicht auf ESM zugreifen.

Einrichten der Zugriffssteuerungsliste (ACL, Access Control List)

Richten Sie eine Liste mit IP-Adressen ein, deren Zugriff auf das ESM-Gerät Sie zulassen oder blockieren möchten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Anmeldesicherheit**.
2. Klicken Sie auf **ACL-Einstellungen**, und fügen Sie dann IP-Adressen zur Liste hinzu.
3. Klicken Sie auf **OK**, um die Einstellungen zu speichern, und schließen Sie die **Zugriffssteuerungsliste**.

Sie können IP-Adressen in der Zugriffssteuerungsliste bearbeiten oder entfernen.

CAC-Einstellungen

Sie können sich gegenüber dem ESM-Gerät authentifizieren, indem Sie über den Browser CAC-Anmeldeinformationen bereitstellen, anstatt einen Benutzernamen und ein Kennwort einzugeben. CACs enthalten ein Client-Zertifikat, durch das der Benutzer identifiziert wird. Dies ist mit der Identifizierung einer Website durch ein Server-Zertifikat vergleichbar. Wenn Sie die CAC-Funktion aktivieren, wird angenommen, dass Sie mit der CAC-basierten Authentifizierung vertraut sind. Sie wissen, in welchen Browsern die Funktionalität unterstützt wird, und sind mit der zu CACs gehörenden EDI-PI (Electronic Data Interchange Personal Identifier) vertraut.

Es kommt vor, dass Zertifikate widerrufen werden. Mithilfe von Zertifikatsperrlisten (Certificate Revocation List, CRL) können Systeme über diese Sperrungen informiert werden. Sie können manuell eine ZIP-Datei mit CRL-Dateien hochladen.

Unter Windows wird ActivClient als einzige CAC-Middleware unterstützt. Wenn Sie unter Windows CAC-Authentifizierung über Internet Explorer in ESM verwenden möchten, muss ActivClient auf dem Client-Computer installiert werden. Nach der Installation von ActivClient werden CAC-Anmeldeinformationen nicht mit dem nativen Smartcard-Manager von Windows, sondern mit ActivClient verwaltet. Wenn über den Client auf andere CAC-fähige Websites zugegriffen wird, ist die ActivClient-Software höchstwahrscheinlich bereits installiert. Anweisungen zum Einrichten von ActivClient und Quellen zum Herunterladen der Software finden Sie unter http://militarycac.com/activclient.htm oder im Intranet Ihres Unternehmens.

Wenn Sie die CAC-Überprüfung für die Authentizität von Anwendungen verwenden, hängt die Sicherheit des Systems von der Sicherheit der Zertifizierungsstelle (Certificate Authority, CA) ab. Bei einer Kompromittierung der Zertifizierungsstelle werden auch CAC-fähige Anmeldungen kompromittiert.

Konfigurieren der CAC-Anmeldung

Zum Einrichten der CAC-Anmeldung müssen Sie die Funktion für die CAC-Anmeldung aktivieren, die Kette der CA-Stammzertifikate hochladen und einen CAC-Benutzer aktivieren, indem Sie den Benutzernamen auf die zehnstellige EDI-PI des Karteninhabers festlegen. Anschließend können Karteninhaber in einem CAC-fähigen Browser auf das ESM-Gerät zugreifen und werden nicht aufgefordert, einen Benutzernamen oder ein Kennwort einzugeben.

ESM umfasst Unterstützung für den Gemalto-Kartenleser. Wenn Sie Hilfe im Zusammenhang mit einem Kartenleser benötigen, wenden Sie sich an den McAfee-Support.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, klicken Sie auf **Anmeldesicherheit**, und wählen Sie dann die Registerkarte **CAC** aus.
2. Geben Sie die Informationen ein, und wählen Sie die erforderlichen Optionen aus. Klicken Sie dann auf **OK**.

3 Aktivieren Sie die einzelnen CAC-Benutzer.

a Klicken Sie in **Systemeigenschaften** auf **Benutzer und Gruppen**, und geben Sie dann das Systemkennwort ein.

b Heben Sie in der Tabelle **Benutzer** den Namen des Benutzers hervor, und klicken Sie dann auf **Bearbeiten**.

c Ersetzen Sie den Namen im Feld **Benutzername** durch die zehnstellige EDI-PI.

d (Optional) Geben Sie den Benutzernamen in das Feld **Benutzer-Alias** ein, und klicken Sie dann auf **OK**.

Konfigurieren von Authentifizierungseinstellungen für Active Directory

Sie können ESM so konfigurieren, dass Benutzer für **Active Directory** authentifiziert werden. Wenn die Funktion aktiviert ist, werden alle Benutzer mit Ausnahme des Systemadministrators über **Active Directory** authentifiziert. Wenn die Authentifizierung deaktiviert ist, können Benutzer, die für die **Active Directory**-Authentifizierung eingerichtet sind, nicht auf das System zugreifen.

Bevor Sie beginnen

- Richten Sie eine **Active Directory**-Instanz ein, auf die über ESM zugegriffen werden kann.
- Erstellen Sie eine Gruppe (siehe *Einrichten von Benutzergruppen*) unter dem Namen der **Active Directory**-Gruppe, die über Zugriff auf ESM verfügt. Wenn Sie beispielsweise der Gruppe den Namen "McAfee-Benutzer" geben, müssen Sie zu **Systemeigenschaften** | **Benutzer und Gruppen** navigieren und eine Gruppe mit dem Namen "McAfee-Benutzer" hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Anmeldesicherheit**.

2 Klicken Sie auf die Registerkarte **Active Directory**, und wählen Sie dann **Active Directory-Authentifizierung aktivieren** aus.

3 Klicken Sie auf **Hinzufügen**, und fügen Sie dann die erforderlichen Informationen zum Einrichten der Verbindung hinzu.

4 Klicken Sie auf der Seite **Active Directory-Verbindung** auf **OK**.

Einrichten von Benutzeranmeldeinformationen für McAfee ePO

Sie können den Zugriff auf ein McAfee ePO-Gerät begrenzen, indem Sie Benutzeranmeldeinformationen festlegen.

Bevor Sie beginnen

Das McAfee ePO-Gerät darf nicht so eingerichtet werden, dass globale Benutzerauthentifizierung erforderlich ist (siehe **Einrichten der globalen Benutzerauthentifizierung**).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf der Systemnavigationsleiste der ESM-Konsole auf **Optionen**, und wählen Sie dann **ePO-Anmeldeinformationen** aus.
2. Klicken Sie auf das Gerät und dann auf **Bearbeiten**.

   Wenn in der Statusspalte für das Gerät **Nicht erforderlich** angezeigt wird, ist das Gerät für globale Benutzerauthentifizierung eingerichtet. Sie können den Status auf der Seite **Verbindung** für das Gerät ändern (siehe *Ändern der Verbindung mit ESM*).

3. Geben Sie den Benutzernamen und das Kennwort ein, testen Sie die Verbindung, und klicken Sie dann auf **OK**.

Für den Zugriff auf dieses Gerät benötigen Benutzer den Benutzernamen und das Kennwort, die Sie hinzugefügt haben.

Deaktivieren oder erneutes Aktivieren eines Benutzers

Wenn die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche innerhalb des unter **Anmeldesicherheit** festgelegten Zeitraums überschritten ist, können Sie das Konto mit dieser Funktion erneut aktivieren. Sie können die Funktion auch verwenden, wenn Sie den Zugriff eines Benutzers vorübergehend oder dauerhaft blockieren müssen, ohne den Benutzer aus dem System zu löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur Folgendes aus: **Systemeigenschaften** | **Benutzer und Gruppen**.
2. Heben Sie in der Tabelle **Benutzer** den Benutzernamen hervor, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie die Option **Konto deaktivieren** aus, oder heben Sie ihre Auswahl auf, und klicken Sie dann auf **OK**.

Das Symbol neben dem Benutzernamen unter in **Benutzer und Gruppen** spiegelt den Status des Kontos wider.

Authentifizieren von Benutzer gegenüber einem LDAP-Server

Sie können ESM so konfigurieren, dass Benutzer gegenüber einem LDAP-Server authentifiziert werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Anmeldesicherheit**.
2. Klicken Sie auf die Registerkarte **LDAP**.
3. Füllen Sie die Felder aus, und klicken Sie dann auf **Anwenden** oder auf **OK**.

Wenn die Option aktiviert ist, müssen sich alle Benutzer mit Ausnahme des Systemadministrators über den LDAP-Server authentifizieren. Wenn die Authentifizierung deaktiviert ist, können Benutzer, die für die LDAP-Authentifizierung eingerichtet sind, nicht auf das System zugreifen.

Einrichten von Benutzergruppen

Gruppen bestehen aus Benutzern, die die Einstellungen der Gruppe erben. Beim Hinzufügen einer Gruppe müssen Geräte, Richtlinien und Berechtigungen zugewiesen werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Benutzer und Gruppen** | **Hinzufügen**.

2 Geben Sie auf den einzelnen Registerkarten die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Die Gruppe wird zur Tabelle **Gruppen** auf der Seite **Benutzer und Gruppen** hinzugefügt.

Hinzufügen einer Gruppe mit eingeschränktem Zugriff

Um den Zugriff bestimmter Benutzer auf die Funktionen des ESM-Geräts einzuschränken, erstellen Sie eine Gruppe, die diese Benutzer enthält. Mit dieser Option schränkten Sie den Zugriff der Benutzer auf Alarme, Fallverwaltung, ELM, Berichte, Watchlists, Ressourcenverwaltung, Richtlinien-Editor, Zonen, Systemeigenschaften, Filter und die Aktionssymbolleiste ein (siehe *Arbeiten mit Benutzern und Gruppen*). Alle anderen Funktionen sind deaktiviert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Benutzer und Gruppen**, und geben Sie dann das Systemkennwort ein.

3 Führen Sie einen der folgenden Schritte aus:

- Wenn die Gruppe bereits eingerichtet ist, wählen Sie sie in der Tabelle **Gruppe** aus, und klicken Sie dann auf **Bearbeiten**.
- Wenn Sie eine Gruppe hinzufügen möchten, klicken Sie neben der Tabelle **Gruppen** auf **Hinzufügen**. Geben Sie Name und Beschreibung ein, und wählen Sie Benutzer aus.

4 Klicken Sie auf **Berechtigungen**, und wählen Sie dann **Zugriff dieser Gruppe einschränken** aus.

Die meisten Berechtigungen sind deaktiviert.

5 Wählen Sie in der Liste der verbleibenden Berechtigungen diejenigen aus, die die Gruppe haben soll.

6 Klicken Sie auf die einzelnen Registerkarten, und definieren Sie die übrigen Einstellungen für die Gruppe.

Sichern und Wiederherstellen von Systemeinstellungen

Sie können die aktuellen Systemkonfigurationseinstellungen automatisch oder manuell speichern, damit sie im Fall eines Systemfehlers oder Datenverlusts wiederhergestellt werden können. Außerdem können Sie die aktuellen Einstellungen auf einem redundanten ESM-Gerät einrichten und speichern. Bei einer Standardsicherung werden alle Konfigurationseinstellungen gesichert, auch die für Richtlinien, sowie SSH-Dateien, Netzwerkdateien und SNMP-Dateien. Wenn Sie ein neues ESM-Gerät hinzufügen, wird die Funktion **Sichern und wiederherstellen** so aktiviert, dass alle sieben Tage eine Sicherung

ausgeführt wird. Sie können vom System empfangene Ereignisse, Flüsse und Protokolle sichern. Bei der ersten Sicherung von Ereignis-, Fluss- oder Protokolldaten werden nur Daten ab dem Anfang des aktuellen Tags gespeichert. Bei den nachfolgenden Sicherungen werden die Daten ab dem Zeitpunkt der letzten Sicherung gespeichert.

Wenn Sie Ereignisse, Flüsse oder Protokolle auf dem ESM-Gerät sichern, wird der Speicherplatz des ESM-Geräts verringert. Es wird empfohlen, regelmäßig Sicherungsdateien vom lokalen ESM-Gerät herunterzuladen oder zu löschen.

Zum Wiederherstellen des Systems können Sie mindestens eine Sicherungsdatei auf dem ESM-Gerät, einem lokalen Computer oder an einem Remote-Speicherort auswählen, um alle Einstellungen und Daten auf einen vorherigen Zustand zurückzusetzen. Wenn Sie diese Funktion verwenden, gehen alle Änderungen verloren, die seit der Erstellung der letzten Sicherung vorgenommen wurden. Wenn Sie beispielsweise eine tägliche Sicherung ausführen und die Daten der letzten drei Tage wiederherstellen möchten, wählen Sie die drei letzten Sicherungsdateien aus. Die Ereignisse, Flüsse und Protokolle aus den drei Sicherungsdateien werden zu den zurzeit auf dem ESM-Gerät vorhandenen Ereignissen, Flüssen und Protokollen hinzugefügt. Dann werden alle Einstellungen mit denen aus der neuesten Sicherung überschrieben.

Sichern von ESM-Einstellungen und Systemdaten

Es gibt mehrere Möglichkeiten zum Sichern der Daten auf dem ESM-Gerät. Wenn Sie ein neues ESM-Gerät hinzufügen, wird die Funktion **Sichern und wiederherstellen** so aktiviert, dass alle sieben Tage eine Sicherung ausgeführt wird. Sie können diese Option deaktivieren oder Änderungen an den Standardeinstellungen vornehmen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Systeminformationen** | **Sichern und wiederherstellen**.
2. Legen Sie die Einstellungen auf eines dieser Elemente fest:
   - Automatische Sicherung
   - Manuelle Sicherung
   - Redundantes ESM-Gerät
   - Wiederherstellen des Systems anhand einer vorherigen Sicherung
3. Klicken Sie auf **OK**, um die Seite **Sichern und wiederherstellen** zu schließen.

Siehe auch

Wiederherstellen der ESM-Einstellungen auf Seite 207
Arbeiten mit Sicherungsdateien in ESM auf Seite 208

Wiederherstellen der ESM-Einstellungen

Nach einem Systemfehler oder Datenverlust können Sie den vorherigen Zustand des Systems wiederherstellen, indem Sie eine Sicherungsdatei auswählen.

Vorgehensweise

Wenn die Datenbank die maximal zulässige Anzahl von Datensätzen enthält und die wiederherzustellen Datensätze sich außerhalb des Bereichs der aktuellen Daten auf dem ESM-Gerät befinden, werden die Datensätze nicht wiederhergestellt. Damit Sie die Daten außerhalb dieses Bereichs speichern und auf sie zugreifen können, muss die Archivierung inaktiver Partitionen eingerichtet sein (siehe *Einrichten von Datenbeibehaltungs-Limits*).

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Systeminformationen** | **Sichern und wiederherstellen** | **Sicherung wiederherstellen**.

2 Wählen Sie den Typ der Wiederherstellung aus, die Sie ausführen möchten.

3 Wählen Sie die wiederherzustellende Datei aus, oder geben Sie die Informationen für den Remote-Speicherort ein. Klicken Sie dann auf **OK**.

Die Wiederherstellung einer Sicherung kann abhängig von der Größe der Wiederherstellungsdatei viel Zeit beanspruchen. Das ESM-Gerät bleibt offline, bis die vollständige Wiederherstellung abgeschlossen ist. In diesem Zeitraum wird alle fünf Minuten versucht, die Verbindung erneut herzustellen. Nach Abschluss des Vorgangs wird die Seite **Anmeldung** angezeigt.

Siehe auch

Einrichten von Datenbeibehaltungs-Limits auf Seite 197

Wiederherstellen gesicherter Konfigurationsdateien

Sie können SSH-, Netzwerk-, SNMP- und andere Konfigurationsdateien wiederherstellen, die für die einzelnen Geräte in ESM gesichert wurden.

Bevor Sie beginnen

Sichern Sie Konfigurationsdateien in ESM (siehe *Sichern von ESM-Einstellungen und Systemdaten*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf die Option **Konfiguration** für das Gerät, auf **Konfiguration wiederherstellen** und dann auf der Bestätigungsseite auf **Ja**.

Arbeiten mit Sicherungsdateien in ESM

Die auf dem ESM-Gerät gespeicherten Sicherungsdateien können heruntergeladen, gelöscht oder angezeigt werden. Außerdem können Sie Dateien hochladen, um sie zur Liste der Sicherungsdateien hinzuzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Dateiwartung**.
2. Wählen Sie in der Dropdown-Liste **Typ auswählen** die Option **Sicherungsdateien** aus.
3. Wählen Sie die auszuführende Aktion aus.
4. Klicken Sie auf **OK**.

Siehe auch

Sichern von ESM-Einstellungen und Systemdaten auf Seite 207

Verwalten der Dateiwartung

Auf dem ESM-Gerät werden Dateien für Sicherungen, Software-Aktualisierungen, Alarmprotokolle und Berichtsprotokolle gespeichert. Sie können aus jeder dieser Listen Dateien herunterladen, hochladen und entfernen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Dateiwartung**.
2. Wählen Sie im Feld **Dateityp auswählen** die Option **Sicherungsdateien**, **Software-Aktualisierungsdateien**, **Alarmprotokolldateien** oder **Berichtsprotokolldateien** aus.
3. Wählen Sie die Dateien aus, und klicken Sie dann auf eine der Optionen.
4. Klicken Sie auf **Anwenden** oder **OK**.

Siehe auch

Sichern von ESM-Einstellungen und Systemdaten auf Seite 207

Redundantes ESM-Gerät

Mit der Funktion Redundantes ESM-Gerät können Sie die aktuellen ESM-Einstellungen auf einem redundanten ESM-Gerät speichern, das im Fall eines Systemfehlers oder Datenverlusts in das primäre ESM-Gerät konvertiert werden kann. Diese Funktion ist nur für Benutzer mit Systemadministrator-Berechtigungen verfügbar.

Wenn Sie ein redundantes ESM-Gerät einrichten, werden die Konfigurations- und Richtliniendaten vom primären ESM-Gerät alle fünf Minuten automatisch mit dem redundanten ESM-Gerät synchronisiert. Zum Einrichten eines redundanten ESM-Geräts müssen Sie die Einstellungen für dieses Gerät, das die Einstellungen und Daten vom primären Gerät erhält, sowie die Einstellungen für das primäre Gerät definieren, von dem die Sicherungseinstellungen und -Daten an das redundante Gerät gesendet werden. Das redundante ESM-Gerät muss bereits konfiguriert sein, damit vom ESM-Gerät eine Verbindung mit ihm hergestellt werden kann.

Die ESM-Redundanzfunktion ist für ESMREC-Kombinationsgeräte nicht verfügbar.

Einrichten eines redundanten ESM-Geräts

Zum Speichern der Systemeinstellungen auf einem redundanten ESM-Gerät müssen Sie beide ESM-Geräte für die Kommunikation miteinander einrichten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Systeminformationen** | **Sichern und wiederherstellen** | **Redundanz**.
2. Stellen Sie sicher, dass im Feld **ESM-Typ** die Option **Primär** ausgewählt ist.
3. Geben Sie die Informationen für das primäre ESM-Gerät ein, und wählen Sie dann die redundanten ESM-Geräte aus, oder fügen Sie sie hinzu.

   Sie können maximal fünf redundante ESM-Geräte hinzufügen.

4. Wählen Sie die Optionsschaltfläche **Redundant** aus, geben Sie dann die IP-Adresse für das primäre ESM-Gerät ein, und wählen Sie den SSH-Port aus.
5. Klicken Sie auf **OK**.

   Sie werden gewarnt, dass der Dienst neu gestartet werden muss und dass dadurch die Verbindungen aller Benutzer mit dem ESM-Gerät getrennt werden.
6. Klicken Sie auf **Ja**, um mit der Synchronisierung fortzufahren.

Ersetzen eines redundanten ESM-Geräts

Wenn ein redundantes ESM-Gerät nicht mehr funktioniert, können Sie es durch ein neues Gerät ersetzen.

Bevor Sie beginnen

Fügen Sie das neue redundante ESM-Gerät zum System hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und vergewissern Sie sich, dass **Systeminformationen** ausgewählt ist.
2. Klicken Sie auf **Sichern und wiederherstellen** | **Redundanz**, und wählen Sie dann **Primär** aus. Geben Sie die neue redundante IP-Adresse in das Feld **IP-Adresse des redundanten ESM-Geräts** ein.
3. Wählen Sie **Redundant** aus, und vergewissern Sie sich, dass die IP-Adresse des primären ESM-Geräts richtig ist.
4. Wählen Sie **Primär** aus, und klicken Sie dann auf **Verbinden**, um zu überprüfen, ob die beiden Geräte kommunizieren.
5. Wählen Sie **Gesamtes ESM-Gerät synchronisieren** aus, und klicken Sie dann auf **OK**.

Verwalten des ESM-Geräts

Sie können verschiedene Vorgänge ausführen, um Software, Protokolle, Zertifikat, Funktionsdateien und Kommunikationsschlüssel für das ESM-Gerät zu verwalten.

Registerkarte	Option	Beschreibung
Konfiguration	**Protokolle verwalten**	Konfigurieren Sie die Ereignistypen, die im Ereignisprotokoll protokolliert werden.
	ESM-Hierarchie	Konfigurieren Sie Datenoptionen, wenn Sie mit hierarchischen ESM-Geräten arbeiten.
	Verschleierung	Definieren Sie globale Einstellungen zum Maskieren ausgewählter Daten in Warnungsdatensätzen, die bei der Ereignisweiterleitung gesendet werden oder an ein übergeordnetes ESM-Gerät gesendet werden.
	Protokollierung	Senden Sie interne Ereignisse zur Speicherung an das ELM-Gerät. Diese Daten können zu Audit-Zwecken verwendet werden.
	Gebietsschema des Systems	Wählen Sie die Systemsprache aus, die für die Protokollierung von Ereignissen verwendet werden soll, beispielsweise für die Integritätsüberwachung und das Geräteprotokoll.
	Namenszuordnung	Heben Sie die Auswahl der Ports und Protokolle auf, damit anstelle von Namen reine Zahlen angezeigt werden. Wenn Sie beispielsweise die Auswahl von **Quellport** oder **Zielport** aufheben, wird *http:80* als *80* angezeigt. Wenn Sie *Protokolle* auswählen, wird die reine Zahl *17* als *udp* angezeigt.
Schlüsselverwaltung	**Zertifikat**	Installieren Sie ein neues SSL-Zertifikat (Secure Socket Layer).
	SSH erneut generieren	Generieren Sie das private oder öffentliche SSH-Schlüsselpaar erneut, um mit allen Geräten zu kommunizieren.
	Alle Schlüssel exportieren	Exportieren Sie die Kommunikationsschlüssel für alle Geräte im System, anstatt die Schlüssel einzeln zu exportieren.
	Alle Schlüssel wiederherstellen	Stellen Sie für alle oder für ausgewählte Geräte die Kommunikationsschlüssel wieder her, die mit der Funktion **Alle Schlüssel exportieren** exportiert wurden.
Wartung	**ESM aktualisieren**	Aktualisieren Sie die ESM-Software über den Regel- und Aktualisierungs-Server von McAfee oder mithilfe eines Sicherheitsmitarbeiters von McAfee.
	ESM-Daten	Laden Sie eine TGZ-Datei mit Informationen zum Status des ESM-Geräts herunter. Diesen Status kann der McAfee-Support bei der Fehlerbehebung und beim Lösen von Problemen verwenden.
	Task-Manager	Zeigen Sie die auf dem ESM-Gerät ausgeführten Abfragen an, und halten Sie sie bei Bedarf an.
	Herunterfahren	Fahren Sie das ESM-Gerät herunter. Sie werden gewarnt, dass durch diese Aktion die Kommunikation aller Benutzer mit dem ESM-Gerät beendet wird.
	Neu starten	Mit dieser Option können Sie das ESM-Gerät anhalten und neu starten. Sie werden gewarnt, dass durch diese Aktion die Kommunikation aller Benutzer mit dem ESM-Gerät beendet wird.

Registerkarte	Option	Beschreibung
	Terminal	Diese Funktion ist nur für fortgeschrittene Benutzer gedacht. Geben Sie Linux-Befehle auf dem ESM-Gerät ein. Da es sich beim Terminal nur um einen teilweisen Batch-Modus-Emulator handelt, stehen nicht alle Befehle zur Verfügung. • Ein vorhandenes Arbeitsverzeichnis wird vom Terminal nicht beibehalten. • Sie können nicht mit `cd` zu einem anderen Verzeichnis wechseln. • Sie müssen vollständige Pfadnamen verwenden. • Die Operatoren > und >> funktionieren nicht. Alle Ergebnisse werden auf dem Bildschirm zurückgegeben.
	Funktionen abrufen	Wenn Sie zusätzliche Funktionen erworben haben, aktivieren Sie diese auf dem ESM-Gerät, indem Sie eine verschlüsselte Datei herunterladen. Die Datei enthält Informationen zu den Funktionen, die von ESM unterstützt werden.
	Funktionen festlegen	Installieren Sie die heruntergeladene Datei mit **Funktionen abrufen**.
	Verbinden	Gewähren Sie dem McAfee-Support bei Support-Anfragen Zugriff auf Ihr System. Diese Option ist nicht FIPS-konform und steht beim Betrieb im FIPS-Modus nicht zur Verfügung.
	Statistik anzeigen	Greifen Sie auf die folgenden Informationen für ESM-Geräte zu: • Statistiken zur Verwendung des Arbeitsspeichers und des Auslagerungsbereichs • CPU-Verwendung • Wechselaktivitäten von Systemen • Statistiken zu Eingang/Ausgang und Übertragungsrate • Länge der Warteschlange und durchschnittliche Belastung

Siehe auch

Zugreifen auf ein Remote-Gerät auf Seite 217
Erneutes Generieren des SSH-Schlüssels auf Seite 215
Verwalten von Empfängern auf Seite 179
Ereignistypen auf Seite 213
Verwalten von Protokollen auf Seite 212
Installieren eines neuen Zertifikats auf Seite 187
Einrichten der ESM-Protokollierung auf Seite 214
Maskieren von IP-Adressen auf Seite 213
Exportieren und Wiederherstellen von Kommunikationsschlüsseln auf Seite 214
Verfügbare Linux-Befehle auf Seite 218
Verwenden von Linux-Befehlen auf Seite 217

Verwalten von Protokollen

Auf dem ESM-Gerät werden verschiedene Ereignistypen generiert. Sie können auswählen, welche Ereignistypen im Ereignisprotokoll gespeichert werden sollen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **ESM-Verwaltung**.

2 Klicken Sie auf **Protokolle verwalten**, und wählen Sie dann die zu protokollierenden Ereignistypen aus.

3 Klicken Sie auf **OK**.

Ereignistypen

Die folgenden Ereignisprotokolltypen werden auf dem ESM-Gerät generiert.

Ereignistyp	Protokollierte Ereignisse
Authentication	Anmeldung, Abmeldung und Änderungen an Benutzerkonten Um die Compliance mit FIPS-Vorschriften zu gewährleisten, ist **Authentifizierungsmodus** immer auf **Keine** festgelegt.
Sicherung	Prozess der Datenbanksicherung
Blacklist	Hierbei handelt es sich um Blacklist-Einträge, die an das Gerät gesendet werden.
Gerät	Änderungen oder Kommunikation bezüglich des Geräts wie der Erhalt von Warnungen, Flüssen oder Protokollen
Ereignisweiterleitung	Änderungen oder Fehler im Zusammenhang mit der Ereignisweiterleitung
Integritätsüberwachung	Ereignisse im Zusammenhang mit dem Gerätestatus
Benachrichtigungen	Änderungen oder Fehler im Zusammenhang mit Benachrichtigungen
Richtlinie	Richtlinienverwaltung und Anwenden von Richtlinien
Regel-Server	Download von Regeln vom Regel-Server und Überprüfung der Regeln Im FIPS-Modus sollten Regeln nicht über den Regel-Server aktualisiert werden.
System	Änderungen an Systemeinstellungen und Protokollierung des Tabellen-Rollovers
Ansichten	Änderungen an Ansichten und Abfragen

Maskieren von IP-Adressen

Sie können auswählen, dass bestimmte Daten in Ereignisdatensätzen, die bei der Ereignisweiterleitung gesendet werden oder an ein übergeordnetes ESM-Gerät gesendet werden, maskiert werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **ESM-Verwaltung** | **ESM-Hierarchie**.

2 Wählen Sie **Verschleiern** für die ESM-Geräte aus, auf denen Sie die Daten maskieren möchten.

Die Seite **Auswahl der zu verbergenden Felder** wird geöffnet.

3 Wählen Sie die Felder aus, die Sie maskieren möchten.

4 Klicken Sie auf **OK**.

Wenn Sie die Funktion eingerichtet haben und von einem übergeordneten ESM-Gerät ein Paket von einem untergeordneten ESM-Gerät angefragt wird, sind die ausgewählten Daten maskiert.

Einrichten der ESM-Protokollierung

Wenn im System ein ELM-Gerät vorhanden ist, können Sie das ESM-Gerät so einrichten, dass die von ihm generierten internen Ereignisdaten an das ELM-Gerät gesendet werden. Dazu müssen Sie den standardmäßigen Protokollierungspool konfigurieren.

Bevor Sie beginnen

Fügen Sie ein ELM-Gerät zum System hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **ESM-Verwaltung**.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Protokollierung**.
3. Wählen Sie die erforderlichen Optionen aus, und klicken Sie dann auf **OK**.

Ändern der Sprache für Ereignisprotokolle

Bei der ersten Anmeldung beim ESM-Gerät haben Sie die Sprache für Ereignisprotokolle wie beispielsweise das Protokoll der Integritätsüberwachung und das Geräteprotokoll ausgewählt. Sie können diese Spracheinstellung ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur Folgendes aus: **Systemeigenschaften** | **ESM-Verwaltung**.
2. Klicken Sie auf **Gebietsschema des Systems**, wählen Sie in der Dropdown-Liste eine Sprache aus, und klicken Sie dann auf **OK**.

Exportieren und Wiederherstellen von Kommunikationsschlüsseln

Exportieren Sie die Kommunikationsschlüssel für alle Geräte im System in eine einzelne Datei. Die exportierten Kommunikationsschlüssel können Sie bei Bedarf wiederherstellen.

- Wählen Sie in der Systemnavigationsstruktur die Optionen **Systemeigenschaften** | **ESM-Verwaltung**aus, und klicken Sie dann auf die Registerkarte **Schlüsselverwaltung**.

Aufgabe	Vorgehensweise
Exportieren aller Kommunikationsschlüssel	1 Klicken Sie auf **Alle Schlüssel exportieren**. 2 Legen Sie das Kennwort für die Schlüsseldatei fest, und klicken Sie dann auf **OK**. 3 Wählen Sie den Speicherort für die Datei aus, und klicken Sie dann auf **Speichern**.
Wiederherstellen aller Kommunikationsschlüssel	1 Klicken Sie auf **Alle Schlüssel wiederherstellen**. 2 Suchen Sie die beim Exportieren der Schlüssel eingerichtete Datei, und klicken Sie dann auf **Öffnen**. 3 Klicken Sie auf **Hochladen**, und geben Sie dann das festgelegte Kennwort ein. 4 Wählen Sie die wiederherzustellenden Geräte aus, und klicken Sie dann auf **OK**.

Erneutes Generieren des SSH-Schlüssels

Generieren Sie das private oder öffentliche SSH-Schlüsselpaar erneut, um mit allen Geräten zu kommunizieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **ESM-Verwaltung**.

2 Klicken Sie auf der Registerkarte **Schlüsselverwaltung** auf **SSH erneut generieren**.

Sie werden gewarnt, dass der alte Schlüssel durch den neuen ersetzt wird.

3 Klicken Sie auf **Ja**.

Wenn der Schlüssel erneut generiert wird, ersetzt er das alte Schlüsselpaar auf allen vom ESM-Gerät verwalteten Geräten.

Task-Manager für Abfragen

Wenn Sie über die Rechte eines Administrators oder Master-Benutzers verfügen, können Sie auf den **Task-Manager** zugreifen. Dort wird die Liste der auf dem ESM-Gerät ausgeführten Abfragen angezeigt. Hier können Sie bestimmte Abfragen schließen, wenn sich diese auf die Systemleistung auswirken. Bei lange ausgeführten Abfragen ist die Wahrscheinlichkeit höher, dass sie sich auf die Leistung auswirken.



Diese Funktion ist für die Fehlerbehebung bei ESM-Laufzeitproblemen gedacht, nicht zum Schließen von Abfragen. Verwenden Sie diese Funktion mit Unterstützung des McAfee-Supports.

Der Task-Manager hat unter anderem folgende Merkmale:

- Sie können Abfragen für Berichte, Ansichten, Watchlists, Ausführungen und Exporte und Alarme sowie Abfragen über externe APIs im System schließen. Systemabfragen können nicht geschlossen werden.
- Wenn Sie auf eine Abfrage klicken, werden die Details im Bereich **Abfragedetails** angezeigt.

- Standardmäßig wird die Liste automatisch alle fünf Sekunden aktualisiert. Wenn Sie eine Abfrage auswählen und die Liste automatisch aktualisiert wird, bleibt die Abfrage ausgewählt, und die Details werden aktualisiert. Wenn die Abfrage abgeschlossen ist, wird sie nicht mehr in der Liste angezeigt.
- Wenn die Liste nicht automatisch aktualisiert werden soll, heben Sie die Auswahl von **Liste automatisch aktualisieren** auf.
- Zum Anzeigen von System-Tasks, das heißt noch nicht identifizierten Tasks, heben Sie die Auswahl von **System-Tasks ausblenden** auf.
- Die Spalten der Tabelle können sortiert werden.
- Sie können die Daten im Bereich **Abfragedetails** auswählen und kopieren.
- Wenn eine Abfrage geschlossen werden kann, wird in der letzten Spalte das Symbol Löschen angezeigt. Wenn Sie auf das Symbol klicken, werden Sie in einem Dialogfeld zur Bestätigung aufgefordert.

Verwalten von Abfragen, die in ESM ausgeführt werden

Im **Task-Manager** wird eine Liste der Abfragen angezeigt, die in ESM ausgeführt werden. Sie können ihren Status anzeigen und Abfragen löschen, die sich auf die Systemleistung auswirken.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften** .
2. Klicken Sie auf **ESM-Verwaltung**, auf die Registerkarte **Wartung** und dann auf **Task-Manager**.
3. Überprüfen Sie die Liste der ausgeführten Abfragen, und führen Sie Aktionen aus.

Aktualisieren eines primären oder redundanten ESM-Geräts

Beim Aktualisieren eines primären oder redundanten ESM-Geräts müssen Sie bestimmte Schritte ausführen, um den Verlust der Ergebnis-, Fluss- und Protokolldaten zu vermeiden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Deaktivieren Sie die Erfassung von Warnungen, Flüssen und Protokollen.
   a. Wählen Sie in der Systemnavigationsstruktur die Option **Systeminformationen** aus, und klicken Sie dann auf **Ereignisse, Flüsse und Protokolle**.
   b. Heben Sie die Auswahl von **Automatische Überprüfung alle** auf.
2. Aktualisieren Sie das primäre ESM-Gerät.
3. Aktualisieren Sie das redundante ESM-Gerät. Wenn Redundanzdateien zu verarbeiten sind, beansprucht der Vorgang mehr Zeit.
4. Aktivieren Sie die Erfassung von Warnungen, Flüssen und Protokollen, indem Sie erneut **Automatische Überprüfung alle** auswählen.

Wenn die Aktualisierung fehlschlägt, finden Sie weitere Informationen unter *Aktualisieren auf Version 9.3*.

Zugreifen auf ein Remote-Gerät

Wenn ein Gerät an einem Remote-Standort eingerichtet ist, können Sie mithilfe der Option **Terminal** Linux-Befehle ausführen, um das Gerät anzuzeigen. Diese Funktion ist für fortgeschrittene Benutzer gedacht und darf nur in Notfällen unter Anleitung von Mitarbeitern des McAfee-Supports verwendet werden.

Diese Option ist nicht FIPS-konform und ist im FIPS-Modus deaktiviert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **ESM-Verwaltung**.
2. Klicken Sie auf der Registerkarte **Wartung** auf **Terminal**.
3. Geben Sie das Systemkennwort ein, und klicken Sie dann auf **OK**.
4. Geben Sie nach Bedarf Linux-Befehle ein, und exportieren Sie den Inhalt zum Speichern in eine Datei.

   Ergebnisse, die während der aktuellen Terminalsitzung auf der Seite **Terminal** gelöscht wurden, sind im Export nicht enthalten.

5. Klicken Sie auf **Schließen**.

Siehe auch

Verfügbare Linux-Befehle auf Seite 218

Verwenden von Linux-Befehlen

Mit der Option **Terminal** können Sie Linux-Befehle auf dem ESM-Gerät eingeben. Diese Funktion ist nur für fortgeschrittene Benutzer gedacht. Verwenden Sie sie nur in Notfällen unter Anleitung des McAfee-Supports.

Diese Option ist nicht FIPS-konform und ist im FIPS-Modus deaktiviert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **ESM-Verwaltung**.
2. Klicken Sie auf der Registerkarte **Wartung** auf **Terminal**, geben Sie das Systemkennwort ein, und klicken Sie dann auf **OK**.
3. Geben Sie Linux-Befehle ein (siehe *Verfügbare Linux-Befehle*).
4. Klicken Sie gegebenenfalls auf **Löschen**, um den Inhalt der Seite zu löschen.
5. (Optional) Klicken Sie auf **Exportieren**, um den Inhalt in einer Datei zu speichern.

   Ergebnisse, die während der aktuellen Terminalsitzung auf der Terminalseite gelöscht wurden, sind im Export nicht enthalten.

Verfügbare Linux-Befehle

Die folgenden Befehle sind auf der Seite **Terminal** verfügbar.

Terminal, Seite, Befehle

- getstatsdata
- ps
- grep
- ifconfig
- kill
- sensors
- service
- cat
- rm
- iptables
- updatedb
- cp
- echo
- date
- ethtool
- df
- tar
- netstat
- sar
- tail
- Suchen
- tcpdump -c -w
- ip6tables

Dies sind die verfügbaren Befehle, die vor der Ausführung geändert werden.

Befehl	Geändert in
II	ll--classify
ping	ping -c 1
ls	ls--classify
top	top -b -n 1
ping6	ping6 -c 1

Informationen zum Befehl getstatsdata finden Sie in Anhang D unter *Sammeln von Statistikdaten für die Fehlerbehebung*. Informationen zu allen anderen Befehlen finden Sie unter http://www.linuxmanpages.com.

Verwenden einer globalen Blacklist

Mit einer Blacklist können Sie den durch ein Nitro IPS-Gerät oder ein virtuelles Gerät fließenden Datenverkehr blockieren, bevor er vom Deep Packet Inspection-Modul analysiert wird.

Mit der Option **Nitro IPS-Blacklist** können Sie eine Blacklist für einzelne Nitro IPS-Geräte auf dem ESM-Gerät einrichten. Mit **Globale Blacklist** können Sie eine Blacklist einrichten, die für alle vom ESM-Gerät verwalteten Nitro IPS-Geräte gilt. Bei dieser Funktion sind nur dauerhafte Blacklist-Einträge zulässig. Zum Einrichten von temporären Einträgen müssen Sie die Option **Nitro IPS-Blacklist** verwenden.

Die globale Blacklist kann von allen Nitro IPS-Geräten und virtuellen Geräten verwendet werden. Die Funktion ist auf allen Geräten deaktiviert, bis Sie sie aktivieren.

Die Seite **Editor für globale Blacklist** enthält drei Registerkarten:

- **Blockierte Quellen**: Ermittelt Übereinstimmungen mit der Quell-IP-Adresse des durch das Gerät geleiteten Datenverkehrs.
- **Blockierte Ziele**: Ermittelt Übereinstimmungen mit der Ziel-IP-Adresse des durch das Gerät geleiteten Datenverkehrs.
- **Ausschlüsse**: Verhindert, dass Datenverkehr automatisch zu einer der Blacklists hinzugefügt wird. Kritische IP-Adressen (z. B. DNS-Server und andere Server oder die Arbeitsstationen von Systemadministratoren) können zu den Ausschlüssen hinzugefügt werden. Dann ist sichergestellt, dass diese ungeachtet der von ihnen generierten Ereignisse nie automatisch in die Blacklist aufgenommen werden.

Sie können Einträge sowohl in **Blockierte Quellen** als auch in **Blockierte Ziele** konfigurieren, um die Auswirkungen der Blacklist auf einen bestimmten Ziel-Port einzuschränken.

Beim Hinzufügen von Einträgen gilt Folgendes:

- **Hinzufügen** ist aktiviert, wenn Sie die IP-Adresse oder den Port ändern.
- Einträge in den Listen **Blockierte Quellen** und **Blockierte Ziele** können so konfiguriert werden, dass Quellen oder Ziele für alle Ports oder für einen bestimmten Port in die Blacklist aufgenommen werden.
- Beim Konfigurieren von Einträgen mit einem maskierten IP-Adressbereich müssen Sie den Port auf Alle (0) und die Dauer auf Dauerhaft festlegen.
- Für diese Listen ist zwar das IP-Adressformat erforderlich, aber es sind einige Tools enthalten, mit denen die Adressen verständlicher gestaltet werden können. Wenn Sie eine IP-Adresse oder einen Hostnamen in das Feld **IP-Adresse** eingegeben haben, wird neben diesem Steuerelement abhängig vom eingegebenen Wert die Schaltfläche **Auflösen** oder **Suche** angezeigt. Wenn der Name der Schaltfläche **Auflösen** lautet und Sie auf die Schaltfläche klicken, wird der eingegebene Hostname aufgelöst, das Feld **IP-Adresse** wird mit diesen Informationen ausgefüllt, und der Hostname wird in das Feld **Beschreibung** verschoben. Wenn Sie dagegen auf **Suche** klicken, wird eine Suche nach der IP-Adresse ausgeführt, und das Feld **Beschreibung** wird mit den Ergebnissen der Suche ausgefüllt.

Manche Websites haben mehrere oder wechselnde IP-Adressen. Daher können Sie sich bei einigen Websites nicht darauf verlassen, dass sie mit diesem Tool zuverlässig blockiert werden.

Einrichten einer globalen Blacklist

Richten Sie eine globale Blacklist ein, die für alle ausgewählten Geräte gilt. So müssen Sie nicht für mehrere Geräte die gleichen Informationen eingeben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Globale Blacklist**.
2. Wählen Sie die Registerkarte **Blockierte Quellen**, **Blockierte Ziele** oder **Ausschlüsse** aus, und verwalten Sie dann Blacklist-Einträge.
3. Wählen Sie die Geräte aus, auf denen die globale Blacklist verwendet werden muss.
4. Klicken Sie auf **Anwenden** oder **OK**.

Was ist Datenanreicherung?

Sie können von Upstream-Datenquellen gesendete Ereignisse mit Kontext anreichern, der im ursprünglichen Ereignis nicht enthalten ist (beispielsweise mit einer E-Mail-Adresse, einer Telefonnummer oder Informationen zum Standort des Hosts). Diese angereicherten Daten werden dann Bestandteil des analysierten Ereignisses und werden genau wie die ursprünglichen Felder mit dem Ereignis gespeichert.

Richten Sie Datenanreicherungsquellen ein, indem Sie definieren, wie die Verbindung mit der Datenbank hergestellt werden soll und auf ein oder zwei Tabellenspalten in der Datenbank zugegriffen werden soll. Legen Sie anschließend fest, welche Geräte die Daten empfangen und wie die Daten (Ereignisse und Flüsse) angereichert werden sollen.

Außerdem können Sie auf der Seite **Datenanreicherung** Datenanreicherungsquellen bearbeiten oder entfernen und eine Abfrage ausführen. Wählen Sie dazu die Quelle aus, und klicken Sie auf **Bearbeiten**, **Entfernen** oder **Jetzt ausführen**.

Im ESM-Gerät ausgelöste Ereignisse werden nicht angereichert. Die Datenerfassung findet in ESM und nicht in den Geräten statt.

Es gibt einen Konnektor für die relationale Datenquelle in Hadoop HBase, von dem die Paare aus Schlüssel und Wert aus der Anreicherungsquelle verwendet werden. Die Identitätszuordnung in HBase kann regelmäßig auf einen Empfänger abgerufen werden, um Ereignisse anzureichern.

Hinzufügen von Datenanreicherungsquellen

Fügen Sie eine Datenanreicherungsquelle hinzu, und legen Sie fest, welche Geräte die Daten empfangen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Datenanreicherung** | **Hinzufügen**.

   Die Registerkarten und Felder in **Datenanreicherungs-Assistent** hängen vom ausgewählten Datenanreicherungstyp ab.

2. Füllen Sie die Felder auf den einzelnen Registerkarten aus, und klicken Sie dann auf **Weiter**.
3. Klicken Sie auf **Fertig stellen** und dann auf **Schreiben**.
4. Wählen Sie die Geräte aus, in die Sie die Datenanreicherungsregeln schreiben möchten, und klicken Sie dann auf **OK**.

Einrichten der Datenanreicherung durch McAfee Real Time for McAfee ePO™

Wenn Sie die McAfee Real Time for McAfee ePO-Quelle im **Datenanreicherungs-Assistenten** auswählen, können Sie Ihre Abfrage testen und die Spalten für **Suche** und **Anreicherung** auswählen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Datenanreicherung**, klicken Sie auf **Hinzufügen**, und geben Sie die Informationen auf der Registerkarte **Hauptbildschirm** ein.
3. Wählen Sie auf der Registerkarte **Quelle** im Feld **Typ** die Option **Real Time for ePO** aus, wählen Sie das Gerät aus, und klicken Sie dann auf die Registerkarte **Abfrage**.
4. Fügen Sie die erforderlichen Informationen hinzu, und klicken Sie anschließend auf **Test**.

Wenn durch die Abfrage nicht die gewünschten Informationen generiert werden, passen Sie die Einstellungen an.

Hinzufügen einer Hadoop HBase-Datenanreicherungsquelle

Rufen Sie HBase-Identitätszuordnungen über einen Empfänger ab, um Ereignisse anzureichern, indem Sie Hadoop HBase als Datenanreicherungsquelle hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Datenanreicherung**.
2. Füllen Sie im **Datenanreicherungs-Assistenten** die Felder auf der Registerkarte **Hauptbildschirm** aus, und klicken Sie dann auf die Registerkarte **Quelle**.
3. Wählen Sie im Feld **Typ** die Option **Hadoop HBase (REST)** aus, und geben Sie dann den Host-Namen, den Port und den Namen der Tabelle ein.
4. Füllen Sie auf der Registerkarte **Abfrage** die Suchspalte und die Informationen für die Abfrage aus:
   a. Verwenden Sie in der **Suchspalte** das Format `spaltenFamilie:spaltenName`.
   b. Füllen Sie die Abfrage mit einem Scanner-Filter aus. Die Werte müssen dabei Base64-codiert sein. Beispiel:

```
<Scanner batch="1024">
<filter>
{
"type": "SingleColumnValueFilter",
"op": "EQUAL",
"family": " ZW1wbG95ZWVJbmZv",
"qualifier": "dXNlcm5hbWU=",
"latestVersion": true,
"comparator": {
"type": "BinaryComparator",
"value": "c2NhcGVnb2F0"
}
}
</filter>
</Scanner>
```

5. Geben Sie die Informationen auf den Registerkarten **Bewertung** und **Ziel** ein.

Hinzufügen einer Hadoop Pig-Datenanreicherungsquelle

Sie können Apache Pig-Abfrageergebnisse nutzen, um Hadoop Pig-Ereignisse anzureichern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus.

2 Klicken Sie auf **Datenanreicherung** und dann auf **Hinzufügen**.

3 Füllen Sie die Felder der Registerkarte **Hauptbildschirm** aus, und klicken Sie dann auf die Registerkarte **Quelle**. Wählen Sie im Feld **Typ** die Option **Hadoop Pig** aus, und geben Sie die folgenden Informationen ein: NameNode-Host, NameNode-Port, JobTracker-Host und JobTracker-Port.



Die JobTracker-Informationen sind nicht erforderlich. Wenn das Feld für die JobTracker-Informationen leer ist, werden NodeName-Host und -Port als Standardeinstellungen verwendet.

4 Wählen Sie auf der Registerkarte **Abfrage** den Modus **Einfach** aus, und geben Sie die folgenden Informationen ein:

a Wählen Sie in **Typ** die Option **Textdatei** aus, und geben Sie in das Feld **Quelle** den Dateipfad ein (beispielsweise `/user/default/Datei.csv`). Wählen Sie alternativ **Hive-Datenbank** aus, und geben Sie eine HCatalog-Tabelle ein (beispielsweise `Probe_07`).

b Geben Sie in **Spalten** an, wie die Spaltendaten angereichert werden sollen.

Wenn die Textdatei beispielsweise Mitarbeiterinformationen mit Spalten für Sozialversicherungsnummer, Name, Geschlecht, Adresse und Telefonnummer enthält, geben Sie in das Feld **Spalten** den folgenden Text ein: `emp_Name:2, emp_phone:5`. Verwenden Sie für Hive-Datenbank die Spaltennamen in der HCatalog-Tabelle.

c In **Filter** können Sie einen beliebigen in Apache Pig integrierten Ausdruck zum Filtern der Daten verwenden. Weitere Informationen finden Sie in der Apache Pig-Dokumentation.

d Wenn Sie oben Spaltenwerte definiert haben, können Sie diese Spaltendaten gruppieren und aggregieren. Hierzu sind Informationen für Quelle und Spalte erforderlich. Die anderen Felder können leer sein. Zum Verwenden von Aggregationsfunktionen müssen Sie Gruppen angeben.

5 Wählen Sie auf der Registerkarte **Abfrage** den Modus **Erweitert** aus, und geben Sie ein Apache Pig-Skript ein.

6 Legen Sie auf der Registerkarte **Bewertung** den Faktor für jeden einzelnen Wert fest, der von der Abfrage für eine einzelne Spalte zurückgegeben wird.

7 Wählen Sie auf der Registerkarte **Ziel** die Geräte aus, auf die Sie die Anreicherung anwenden möchten.

Hinzufügen von Active Directory-Datenanreicherung für Benutzernamen

Sie können Microsoft Active Directory nutzen, um Windows-Ereignisse mit den vollständigen Anzeigenamen der Benutzer auszufüllen.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie über die Berechtigung zur Systemverwaltung verfügen.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus.

2 Klicken Sie auf **Datenanreicherung** und dann auf **Hinzufügen**.

3 Geben Sie auf der Registerkarte **Hauptbildschirm** einen aussagekräftigen Namen unter **Anreicherungsname** ein. Verwenden Sie dabei das Format `Vollständiger_Name_aus_Benutzer-ID`.

4 Legen Sie **Suchtyp** und **Anreicherungstyp** auf **Zeichenfolge** fest.

5 Legen Sie **Abrufhäufigkeit** auf **täglich** fest, sofern Active Directory nicht häufiger aktualisiert wird.

6 Klicken Sie auf **Weiter** oder auf die Registerkarte **Quelle**.

   a Wählen Sie im Feld **Typ** die Option **LDAP** aus.

   b Geben Sie IP-Adresse, Benutzername und Kennwort ein.

7 Klicken Sie auf **Weiter** oder auf die Registerkarte **Abfrage**.

   a Geben Sie in das Feld **Suchattribut** die Zeichenfolge `sAMAccountName` ein.

   b Geben Sie in das Feld **Anreicherungsattribut** die Zeichenfolge `displayName` ein.

   c Geben Sie in das Feld **Abfrage** die Zeichenfolge `(objectClass=person)` ein, um eine Liste aller als Person klassifizierten Objekte in Active Directory zurückzugeben.

   d Testen Sie die Abfrage. Dabei werden ungeachtet der Anzahl der tatsächlichen Einträge maximal fünf Werte zurückgegeben.

8 Klicken Sie auf **Weiter** oder auf die Registerkarte **Ziel**.

   a Klicken Sie auf **Hinzufügen**.

   b Wählen Sie die Microsoft Windows-Datenquelle aus.

   c Wählen Sie im **Suchfeld** das Feld **Quellbenutzer** aus.

   Dieses Feld entspricht dem Wert aus dem Ereignis, das als Index für die Suche verwendet wird.

   d Wählen Sie das **Anreicherungsfeld** aus. Dort wird der Anreicherungswert im Format `Benutzerspitzname` oder `Kontaktname` angegeben.

9 Klicken Sie auf **Fertig stellen**, um die Eingaben zu speichern.

10 Klicken Sie nach dem Schreiben der Anreicherungseinstellungen in die Geräte auf **Jetzt ausführen**, um die Anreicherungswerte aus der Datenquelle abzurufen, bis der Wert **Tägliche Auslösungszeit** gefunden wird.

Der **vollständige Name** wird in das Feld **Contact_name** geschrieben.

4 Verwalten von Cyber-Bedrohungen

Sie können mit McAfee ESM Kompromittierungsindikatoren (Indicators of Compromise, IOC) aus Remote-Quellen abrufen und schnell auf zugehörige IOC-Aktivitäten in Ihrer Umgebung zugreifen.

Durch die Verwaltung von Cyber-Bedrohungen können Sie automatische Feeds einrichten, durch die Watchlists, Alarme und Berichte generiert werden. Auf diese Weise erhalten Sie Einblicke in Daten, für die Sie Maßnahmen ergreifen können. Sie können beispielsweise einen Feed einrichten, durch den automatisch verdächtige IP-Adressen zu Watchlists hinzugefügt werden, um zukünftigen Datenverkehr zu überwachen. Durch diesen Feed können Berichte zu vergangenen Aktivitäten generiert und gesendet werden. Mit den Optionen **Workflow-Ansichten für Ereignisse > Cyber Threat-Indikatoren** können Sie schnell bestimmte Ereignisse und Aktivitäten in der Umgebung weiter aufgliedern.

Inhalt

- *Einrichten der Cyber Threat-Verwaltung*
- *Anzeigen von Ergebnissen eines Cyber Threat-Feeds*

Einrichten der Cyber Threat-Verwaltung

Richten Sie Feeds ein, um Kompromittierungsindikatoren (Indicators of Compromise, IOC) aus Remote-Quellen abzurufen. Mithilfe dieser Feeds können Sie Watchlists, Alarme und Berichte generieren, damit Benutzer auf zugehörige IOC-Aktivitäten in Ihrer Umgebung zugreifen können.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie über die folgenden Berechtigungen verfügen:

- Cyber Threat-Verwaltung: Ermöglicht Benutzern das Einrichten eines Cyber Threat-Feeds.
- Cyber Threat-Benutzer: Ermöglicht Benutzern das Anzeigen der durch den Feed generierten Daten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Systemnavigationsstruktur auf **Systemeigenschaften**.
2. Klicken Sie auf **Cyber Threat-Feeds** und dann auf **Hinzufügen**.
3. Geben Sie auf der Registerkarte **Hauptbildschirm** den Feed-Namen ein.
4. Wählen Sie auf der Registerkarte **Quelle** den Quelldatentyp und die Anmeldeinformationen für die Verbindung aus. Klicken Sie auf **Verbinden**, um die Verbindung zu testen.



Als Quellen werden unter anderem McAfee Advanced Threat Defense und MITRE Threat Information Exchange (TAXII) unterstützt.

5 Legen Sie auf der Registerkarte **Häufigkeit** fest, wie oft die IOC-Dateien für den Feed abgerufen werden sollen (Abrufhäufigkeit). Für die Abrufhäufigkeit sind folgende Einstellungen möglich: alle x Minuten, täglich, stündlich, wöchentlich oder monatlich. Legen Sie die tägliche Auslösungszeit fest.

6 Wählen Sie auf der Registerkarte **Watchlist** aus, welche Eigenschaft bzw. welches Feld einer IOC-Datei an eine vorhandene Watchlist angefügt werden soll. Sie können Watchlists für alle unterstützten Eigenschaften oder Felder hinzufügen.

Wenn die benötigte Watchlist noch nicht vorhanden ist, klicken Sie auf **Neue Watchlist erstellen**.

7 Legen Sie auf der Registerkarte **Rückverfolgung** fest, welche Ereignisse (Standard) und Flüsse analysiert werden sollen, welche übereinstimmenden Daten analysiert werden sollen und für welchen Zeitraum in der Vergangenheit die Daten anhand dieses Feeds analysiert werden sollen.

a Wählen Sie aus, ob Ereignisse und/oder Flüsse analysiert werden sollen.

b Geben Sie an, für welchen Zeitraum in der Vergangenheit (in Tagen) die Ereignisse und Flüsse analysiert werden sollen.

c Legen Sie fest, welche Aktion von ESM ausgeführt werden soll, wenn bei der Rückverfolgung eine Datenübereinstimmung gefunden wird.

d Wählen Sie für Alarme einen Beauftragten und einen Schweregrad aus.

8 Kehren Sie zur Registerkarte **Hauptbildschirm** zurück, und wählen Sie dann **Aktiviert** aus, um den Feed zu aktivieren.

9 Klicken Sie auf **Fertig stellen**.

Siehe auch

Anzeigen von Ergebnissen eines Cyber Threat-Feeds auf Seite 226

Anzeigen von Ergebnissen eines Cyber Threat-Feeds

Zeigen Sie Kompromittierungsindikatoren (Indicators of Compromise, IOC) aus externen Datenquellen an, die durch die Cyber Threat-Feeds Ihres Unternehmens identifiziert werden. Sie können schnell die Bedrohungsdetails, Dateibeschreibungen und entsprechenden Ereignisse für die einzelnen Indikatorquellen weiter aufgliedern.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie über die Berechtigung Cyber Threat-Benutzer verfügen, mit der Sie die Ergebnisse der Cyber Threat-Feeds des Unternehmens anzeigen können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der ESM-Konsole unter **Standardübersicht** die Optionen **Workflow-Ansichten für Ereignisse | Cyber Threat-Indikatoren** aus.

2 Wählen Sie den Zeitraum für die Ansicht aus.

3 Filtern Sie nach Feed-Namen oder unterstützten IOC-Datentypen.

4 Führen Sie eine der folgenden Standardaktionen für die Ansicht aus:
- Watchlist erstellen oder an eine Watchlist anfügen
- Alarm erstellen
- Remote-Befehl ausführen
- Fall erstellen
- Umliegende Ereignisse untersuchen oder Letzte Untersuchung der umliegenden Ereignisse
- Indikator in eine CSV- oder HTML-Datei exportieren

5 Aufgliedern der Bedrohungsdetails mithilfe der Registerkarten **Beschreibung**, **Details**, **Quellereignisse** und **Quellflüsse**

Siehe auch
Einrichten der Cyber Threat-Verwaltung auf Seite 225

5 Arbeiten mit Inhaltspaketen

Bei Auftreten konkreter Bedrohungssituationen können Sie sofort reagieren, indem Sie die entsprechenden Inhaltspakete vom Regel-Server importieren und installieren. Inhaltspakete enthalten auf Verwendungsszenarien abgestimmte Korrelationsregeln, Alarme, Ansichten, Berichte, Variablen und Watchlists für die Behandlung bestimmter Malware-Aktivitäten oder Bedrohungsaktivitäten. Mithilfe von Inhaltspaketen können Sie auf Bedrohungen reagieren, ohne Zeit damit zu verlieren, Tools von Grund auf zu erstellen.

Importieren von Inhaltspaketen

McAfee erstellt auf Verwendungsszenarien abgestimmte Inhaltspakete mit Korrelationsregeln, Alarmen, Ansichten, Berichten, Variablen oder Watchlists für die Behandlung bestimmter Malware-Aktivitäten.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie über die folgenden Berechtigungen verfügen:

- Systemverwaltung
- Benutzerverwaltung

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Überprüfen auf Regelaktualisierungen auf Seite 24

> Online-Benutzer erhalten verfügbare Inhaltspakete automatisch im Rahmen von Regelaktualisierungen. Offline-Benutzer müssen einzelne Inhaltspakete manuell von der Hosting-Site für Regeln herunterladen.

2 Klicken Sie in der Systemnavigationsstruktur auf **Systemeigenschaften**.

3 Klicken Sie auf **Inhaltspakete**.

4 Zum Importieren und Installieren eines neuen Inhaltspakets klicken Sie auf **Durchsuchen**.

> Bei der Überprüfung auf Regelaktualisierungen werden automatisch neue oder aktualisierte Inhaltspakete heruntergeladen.

a Klicken Sie auf **Importieren**, und navigieren Sie zu der Inhaltspaketdatei, die Sie importieren möchten.

b Klicken Sie auf **Hochladen**.

Der Status des Imports wird in einer Meldung angezeigt.

c Klicken Sie auf das Inhaltspaket, um die Details zum Inhalt des Pakets anzuzeigen.

d Wählen Sie das gewünschte Paket aus, und wählen Sie dann die Option zum Installieren des Inhaltspakets aus.

5 Zum Aktualisieren oder Deinstallieren eines vorhandenen Inhaltspakets aktivieren Sie das Kontrollkästchen des gewünschten Pakets, und klicken Sie auf **Aktualisieren** oder **Deinstallieren**.



Seien Sie vorsichtig, wenn Sie vorhandene Inhaltspakete aktualisieren. Wenn Sie Elemente von Inhaltspaketen angepasst haben, werden diese angepassten Elemente möglicherweise bei der Aktualisierung überschrieben.

6 Zum Deinstallieren eines vorhandenen Inhaltspakets aktivieren Sie das Kontrollkästchen des gewünschten Pakets, und klicken Sie auf **Deinstallieren**.

6 Arbeiten mit Alarmen

Inhalt

- *Funktionsweise der ESM-Alarme*
- *Erstellen eines Alarms*
- *Aktivieren oder Deaktivieren der Alarmüberwachung*
- *Anpassen der Übersicht für ausgelöste Alarme und Fälle*
- *Verwalten von Nachrichtenvorlagen für Alarme*
- *Verwalten von Audiodateien für Alarme*
- *Verwalten von Alarmempfängern*
- *Verwalten von Alarmen*

Funktionsweise der ESM-Alarme

Sie können das System so konfigurieren, dass Alarme in Echtzeit bereitgestellt werden.

Ein ausgelöster Alarm wird automatisch zum Protokoll **Alarme** (unter der Systemnavigationsstruktur) sowie zur Ansicht **Ausgelöste Alarme** hinzugefügt. Außerdem können Sie Alarmaktionen für folgende Zwecke konfigurieren:

- Protokollieren eines Ereignisses in ESM
- Bereitstellen einer visuellen und akustischen Warnung
- Erstellen eines Falls für eine bestimmte Person oder Gruppe
- Ausführen eines Skripts
- Aktualisieren einer Watchlist
- Senden eines Ereignisses an Remedy
- Senden einer SMS oder E-Mail

Im Protokollbereich **Alarme** wird die Gesamtanzahl der zurzeit aufgeführten Alarme nach Schweregrad angezeigt:

Symbol	Schweregrad	Bereich
	Hoch	66–100
	Mittel	33–65
	Niedrig	1–32

Ein hinzugefügter Alarm wird ausgelöst, wenn die Bedingungen zutreffen. Wenn Sie die **Maximale Häufigkeit der Bedingungsauslösung** auf 15 Minuten festlegen, wird der Alarm erstmals ausgelöst, wenn die im Feld **Ereignisanzahl** angegebene Ereignisanzahl innerhalb eines Zeitraums von 15 Minuten auftritt. Durch in den ersten 15 Minuten eingehende Ereignisse wird der Alarm nicht ausgelöst.

Sie können die ausgelösten Alarme bestätigen, löschen und Details zu ihnen anzeigen. Wenn Sie einen ausgelösten Alarm bestätigen, wird er im Protokoll **Alarme** nicht mehr angezeigt. In der Ansicht **Ausgelöste Alarme** wird er jedoch nach wie vor aufgeführt. Wenn Sie einen Alarm löschen, wird er aus dem Protokoll **Alarme** sowie aus der Ansicht **Ausgelöste Alarme** entfernt.

Wenn Sie auf der Seite **Alarmeinstellungen** die Aktion **Visuelle Warnung** auswählen und die Warnung nicht geschlossen, bestätigt oder gelöscht wurde, wird die visuelle Warnung nach 30 Sekunden geschlossen. Die ausgewählte Audiowarnung wird wiedergegeben, bis Sie die visuelle Warnung schließen, bestätigen oder löschen oder auf das Audiosymbol klicken, um die Audiowarnung zu beenden.

Sie können auswählen, ob der Protokollbereich **Alarme** auf der Seite **Optionen** angezeigt werden soll (siehe *Auswählen von Benutzereinstellungen*).

Siehe auch

Auswählen von Benutzereinstellungen auf Seite 30

Erstellen eines Alarms

Fügen Sie einen Alarm hinzu, damit er ausgelöst wird, wenn die von Ihnen definierten Bedingungen zutreffen.

Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen oder einer Zugriffsgruppe mit der Berechtigung **Alarmverwaltung** angehören.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Alarme** | **Hinzufügen**.

2 Geben Sie die Informationen auf den Registerkarten **Zusammenfassung**, **Bedingung**, **Aktionen** und **Eskalation** ein.

Unter *UCAPL-Alarme* finden Sie eine Liste und Beschreibung der Alarme, die Ihnen helfen soll, UCAPL-Anforderungen (Unified Capabilities Approved Products List) zu erfüllen.

3 Klicken Sie auf **Fertig stellen**.

Der Alarm wird der Liste auf der Seite **Alarme** hinzugefügt und ausgelöst, wenn die Bedingungen zutreffen.

Aufgaben

- *Einrichten eines Korrelationsalarms, der Quellereignisse enthalten soll* auf Seite 235
  Wenn Sie Tags zu einem Alarm vom Typ **Interne Ereignisübereinstimmung** hinzufügen, bei dem ein Korrelationsereignis als Übereinstimmung verwendet wird, enthalten die Ergebnisse Informationen zu den Quellereignissen.
- *Hinzufügen eines Alarms vom Typ Feldübereinstimmung* auf Seite 236
  Bei einem Alarm vom Typ **Feldübereinstimmung** liegt eine Übereinstimmung mit mehreren Feldern eines Ereignisses vor. Der Alarm wird ausgelöst, sobald das Ereignis vom Gerät empfangen und analysiert wird.
- *Hinzufügen eines Alarms zu Regeln* auf Seite 237
  Sie können zu bestimmten Regeln einen Alarm hinzufügen, damit Sie benachrichtigt werden, wenn Ereignisse durch diese Regeln generiert werden.
- *Erstellen eines SNMP-Traps als Aktion in einem Alarm* auf Seite 189
  Sie können SNMP-Traps als Aktion innerhalb eines Alarms senden.
- *Hinzufügen eines Alarms zur Benachrichtigung bei Stromausfällen* auf Seite 190
  Fügen Sie einen Alarm hinzu, damit Sie bei Ausfall einer der ESM-Stromversorgungen benachrichtigt werden.
- *Hinzufügen eines Alarms für Integritätsüberwachungsereignisse* auf Seite 239
  Durch Integritätsüberwachungsregeln werden Ereignisse generiert, die unter einem Basisgerät in der Systemnavigationsstruktur angezeigt werden.
- *Kopieren eines Alarms* auf Seite 247
  Sie können einen vorhandenen Alarm als Vorlage für einen neuen Alarm verwenden, indem Sie den Alarm kopieren und unter einem anderen Namen speichern.

UCAPL-Alarme

Sie können verschiedene Alarmtypen hinzufügen, um UCAPL-Anforderungen zu erfüllen.

Informationen zum Einrichten der allgemeinen Alarmeinstellungen finden Sie unter *Erstellen eines Alarms*. Führen Sie dann die Schritte in dieser Tabelle aus.

Alarmtyp	Beschreibung
Anpassbarer Schwellenwert für fehlgeschlagene Anmeldungen erreicht	Zum Auslösen eines Alarms bei Erreichen eines anpassbaren Schwellenwerts für die Anzahl fehlgeschlagener Anmeldungen durch den gleichen Benutzer erstellen Sie einen Alarm vom Typ **Interne Ereignisübereinstimmung** mit Vergleich der **Signatur-ID**, und geben Sie den Wert `306-36` ein.
Schwellenwert für Zeitraum ohne Aktivität erreicht	Zum Auslösen eines Alarms bei Sperrung eines Benutzerkontos aufgrund des erreichten Schwellenwerts für einen Zeitraum ohne Aktivität erstellen Sie einen Alarm vom Typ **Interne Ereignisübereinstimmung** mit Vergleich der **Signatur-ID**, und geben Sie den Wert `306-35` ein.
Anzahl von zulässigen gleichzeitigen Sitzungen erreicht	Zum Auslösen eines Alarms beim Versuch eines Benutzers, sich nach Erreichen der Anzahl von zulässigen gleichzeitigen Sitzungen anzumelden, erstellen Sie einen Alarm vom Typ **Interne Ereignisübereinstimmung** mit Vergleich der **Signatur-ID**, und geben Sie den Wert `306-37` ein.
Fehlgeschlagene Integritätsprüfung für Systemdateien	Zum Auslösen eines Alarms bei einer fehlgeschlagenen Integritätsprüfung für Systemdateien erstellen Sie einen Alarm vom Typ **Interne Ereignisübereinstimmung** mit Vergleich der **Signatur-ID**, und geben Sie den Wert `306-50085` ein.

Alarmtyp	Beschreibung
Zertifikate laufen in Kürze ab	Zum Auslösen eines Alarms bei bevorstehendem Ablauf von CAC-Zertifikaten (Common Access Card) oder Web-Server-Zertifikaten erstellen Sie einen Alarm vom Typ **Interne Ereignisübereinstimmung** mit Vergleich der **Signatur-ID**, und geben Sie den Wert `306-50081`, `306-50082`, `306-50083`, `306-50084` ein. Der Alarm wird 60 Tage vor Ablauf und anschließend wöchentlich ausgelöst. Die Anzahl der Tage kann zurzeit nicht konfiguriert werden.
SNMP-Trap gesendet bei nicht genehmigtem Systemstatus	Wenn Sie einen SNMP-Trap als Alarmaktion konfigurieren möchten, damit ein Trap an NMS gesendet wird, wenn erkannt wird, dass sich das System nicht mehr in einem genehmigten oder sicheren Zustand befindet, führen Sie die folgenden Schritte aus: **1** Erstellen Sie einen Alarm mit Vergleich einer beliebigen Bedingung. Wechseln Sie dann zur Registerkarte **Aktionen**, und wählen Sie **Nachricht senden** aus. **2** Klicken Sie auf **Empfänger hinzufügen** | **SNMP**, wählen Sie den Empfänger aus, und klicken Sie dann auf **OK**. **3** Klicken Sie im Feld **Nachricht senden** auf **Konfigurieren**, klicken Sie auf **Vorlagen** und dann auf **Hinzufügen**. **4** Wählen Sie im Feld **Typ** die Option **SNMP-Vorlage** aus, geben Sie den Text für die Nachricht ein, und klicken Sie dann auf **OK**. **5** Wählen Sie auf der Seite **Vorlagenverwaltung** die neue Vorlage aus, und klicken Sie dann auf **OK**. **6** Füllen Sie die verbleibenden Alarmeinstellungen aus.
Syslog-Nachricht gesendet bei nicht genehmigtem Systemstatus	Wenn Sie eine Syslog-Nachricht als Alarmaktion konfigurieren möchten, damit eine Syslog-Nachricht an NMS gesendet wird, wenn erkannt wird, dass sich das System nicht mehr in einem genehmigten oder sicheren Zustand befindet, führen Sie die folgenden Schritte aus: **1** Erstellen Sie einen Alarm mit Vergleich einer beliebigen Bedingung. Wechseln Sie zur Registerkarte **Aktionen**, und wählen Sie dann **Nachricht senden** aus. **2** Klicken Sie auf **Empfänger hinzufügen** | **Syslog**, wählen Sie den Empfänger aus, und klicken Sie dann auf **OK**. **3** Klicken Sie im Feld **Nachricht senden** auf **Konfigurieren**, klicken Sie dann auf **Vorlagen** und auf **Hinzufügen**. **4** Wählen Sie im Feld **Typ** die Option **Syslog-Vorlage** aus, geben Sie den Text für die Nachricht ein, und klicken Sie dann auf **OK**. **5** Wählen Sie auf der Seite **Vorlagenverwaltung** die neue Vorlage aus, und klicken Sie dann auf **OK**. **6** Füllen Sie die verbleibenden Alarmeinstellungen aus.

Alarmtyp	Beschreibung
Erforderliche Ereignisse werden im Sicherheitsprotokoll nicht aufgezeichnet	Zum Konfigurieren eines SNMP-Traps, der innerhalb von 30 Sekunden an ein entsprechendes Netzwerkbetriebszentrum (Network Operation Center, NOC) gesendet wird, wenn erforderliche Ereignisse nicht im Sicherheitsprotokoll aufgezeichnet werden, führen Sie die folgenden Schritte aus: 1 Wechseln Sie zu **Systemeigenschaften** | **SNMP-Konfiguration** | **SNMP-Traps** oder **Geräteeigenschaften** | **Gerätekonfiguration** | **SNMP**. 2 Wählen Sie den Trap für Fehler im Sicherheitsprotokoll aus, konfigurieren Sie dann mindestens ein Profil, an das die Traps gesendet werden sollen, und klicken Sie auf **Anwenden**. Die SNMP-Traps werden mit der Nachricht "Das Schreiben in das Sicherheitsprotokoll ist fehlgeschlagen" an den SNMP-Profilempfänger gesendet.
Audit-Funktionen werden gestartet oder heruntergefahren	Zum Konfigurieren eines SNMP-Traps, der beim Starten oder Herunterfahren der Audit-Funktionen (beispielsweise database, cpservice, IPSDBServer) gesendet wird, greifen Sie auf **SNMP-Traps** oder **SNMP-Einstellungen** zu (siehe vorheriges Element), und wählen Sie **Traps für Datenbank aktiv/inaktiv** aus. Konfigurieren Sie mindestens ein Profil, an das die Traps gesendet werden sollen, und klicken Sie auf **Anwenden**.
Sitzung für jede administrative Rolle vorhanden	Zum Auslösen eines Alarms bei Vorhandensein einer administrativen Sitzung für jede der definierten administrativen Rollen erstellen Sie einen Alarm vom Typ **Interne Ereignisübereinstimmung** mit Vergleich der **Signatur-ID**, und geben Sie die Werte 306-38 für Audit-Administrator, 306-39 für Kryptografie-Administrator und 306-40 für Power-User ein. Sie können auch separate Alarme einrichten.

Siehe auch

Erstellen eines Alarms auf Seite 232

Einrichten eines Korrelationsalarms, der Quellereignisse enthalten soll

Wenn Sie Tags zu einem Alarm vom Typ **Interne Ereignisübereinstimmung** hinzufügen, bei dem ein Korrelationsereignis als Übereinstimmung verwendet wird, enthalten die Ergebnisse Informationen zu den Quellereignissen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

2 Klicken Sie auf **Alarme**, auf die Registerkarte **Einstellungen** und dann auf **Vorlagen**.

3 Klicken Sie auf der Seite **Vorlagenverwaltung** auf **Hinzufügen**, und geben Sie dann die erforderlichen Informationen ein.

4 Platzieren Sie im Abschnitt **Nachrichtentext** den Cursor an der Stelle, an der Sie die Tags einfügen möchten. Klicken Sie dann auf das Symbol **Feld einfügen** , und wählen Sie **Quellereignisblock** aus.

5 Platzieren Sie den Cursor zwischen den Tags, und klicken Sie erneut auf das Symbol **Feld einfügen**. Wählen Sie dann die Informationen aus, die Sie beim Auslösen des Korrelationsalarms einschließen möchten.

Das Feld Nachrichtentext sieht wie im folgenden Beispiel aus, wenn Sie Quell-IP, Ziel-IP und Schweregrad des Ereignisses in die Nachricht einschließen:

Alarm: [$Alarm Name]
Beauftragter: [$Alarm Assignee]
Auslösungsdatum: [$Trigger Date] Zusammenfassung: [$Alarm Summary]
[$SOURCE_EVENTS_START] Quell-IP: [$Source IP]
Ziel-IP: [$Destination IP]
Schweregrad: [$Average Severity]
[$SOURCE_EVENTS_END]

Wenn der Alarm nicht von einem korrelierten Ereignis ausgelöst wird, enthält die Nachricht die Daten nicht.

Hinzufügen eines Alarms vom Typ Feldübereinstimmung

Bei einem Alarm vom Typ **Feldübereinstimmung** liegt eine Übereinstimmung mit mehreren Feldern eines Ereignisses vor. Der Alarm wird ausgelöst, sobald das Ereignis vom Gerät empfangen und analysiert wird.

Die bisherige Alarmbedingung **Feldübereinstimmung** heißt jetzt **Interne Ereignisübereinstimmung**.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System aus. Klicken Sie auf das Symbol **Eigenschaften** und dann auf **Alarme**.

2 Klicken Sie auf **Hinzufügen**, geben Sie den Alarmnamen ein, wählen Sie den Beauftragten aus, und klicken Sie dann auf die Registerkarte **Bedingung**.

3 Wählen Sie im Feld **Typ** die Option **Feldübereinstimmung** aus, und richten Sie dann die Bedingungen für den Alarm ein.

   a Ziehen Sie das Symbol **UND** oder **ODER** (siehe *Logische Elemente* im Produkthandbuch), und legen Sie es an der gewünschten Stelle ab, um die Logik für die Bedingung des Alarms einzurichten.

   b Ziehen Sie das Symbol **Komponente vergleichen** auf das logische Element, legen Sie es ab, und füllen Sie dann die Seite **Filterfeld hinzufügen** aus.

   c Wählen Sie im Feld **Maximale Häufigkeit der Bedingungsauslösung** aus, wie viel Zeit zwischen den einzelnen Bedingungen verstreichen muss. Damit verhindern Sie eine Flut von Benachrichtigungen. Jeder Auslöser enthält nur das erste Quellereignis, das der Auslösebedingung entspricht, nicht jedoch die Ereignisse, die innerhalb des Zeitraums für die Bedingungsauslösung aufgetreten sind. Durch neue Ereignisse, die der Auslösebedingung entsprechen, wird der Alarm nicht erneut ausgelöst, sondern erst nach dem maximalen Zeitraum für die Bedingungsauslösung.

   Wenn Sie den Zeitraum auf null festlegen, wird durch alle Ereignisse ein Alarm generiert.

4 Klicken Sie auf **Weiter**, und wählen Sie die Geräte aus, die für diesen Alarm überwacht werden sollen. Dieser Alarmtyp unterstützt Empfänger, lokale Empfänger-ELM-Geräte (Enterprise Log Manager), Kombinationen aus Empfänger und ELM, ACE-Geräte und ADM-Geräte (Application Data Monitor).

5 Klicken Sie auf die Registerkarten **Aktionen** und **Eskalation**, und definieren Sie die Einstellungen. Klicken Sie dann auf **Fertig stellen**.

Der Alarm wird in das Gerät geschrieben.

Wenn der Alarm nicht in das Gerät geschrieben wird, geht aus einer Kennzeichnung neben dem Gerät in der Systemnavigationsstruktur hervor, dass das Gerät nicht synchronisiert ist. Klicken Sie auf die Kennzeichnung und dann auf **Alarme synchronisieren**.

Hinzufügen eines Alarms zu Regeln

Sie können zu bestimmten Regeln einen Alarm hinzufügen, damit Sie benachrichtigt werden, wenn Ereignisse durch diese Regeln generiert werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der Systemnavigationsstruktur auf der Aktionssymbolleiste auf das Symbol **Richtlinien-Editor** .

2 Wählen Sie im Bereich **Regeltypen** den Typ der Regel aus.

3 Wählen Sie im Anzeigebereich für Regeln mindestens eine Regel aus.

4 Klicken Sie auf das Symbol **Alarme** .

5 Legen Sie die Einstellungen für den Alarm fest.

Siehe auch

Erstellen eines Alarms auf Seite 232

Erstellen eines SNMP-Traps als Aktion in einem Alarm

Sie können SNMP-Traps als Aktion innerhalb eines Alarms senden.

Bevor Sie beginnen

Bereiten Sie den SNMP-Trap-Empfänger vor (nur erforderlich, wenn kein SNMP-Trap-Empfänger vorhanden ist).

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

Vorgehensweise

1 Erstellen Sie ein SNMP-Profil, um für ESM anzugeben, wohin die SNMP-Traps gesendet werden sollen.

a Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften** .

b Klicken Sie auf **Profilverwaltung**, und wählen Sie dann im Feld **Profiltyp** die Option **SNMP-Trap** aus.

c Füllen Sie die verbleibenden Felder aus, und klicken Sie dann auf **Anwenden**.

2 Konfigurieren Sie SNMP in ESM.

   a Klicken Sie in **Systemeigenschaften** auf **SNMP-Konfiguration** und dann auf die Registerkarte **SNMP-Traps**.

   b Wählen Sie den Port aus, wählen Sie die Trap-Typen aus, die gesendet werden sollen, und wählen Sie dann das in Schritt 1 hinzugefügte Profil aus.

   c Klicken Sie auf **Anwenden**.

3 Definieren Sie einen Alarm mit der Aktion **SNMP-Trap**.

   a Klicken Sie in **Systemeigenschaften** auf **Alarme** und dann auf **Hinzufügen**.

   b Geben Sie auf den Registerkarten **Zusammenfassung**, **Bedingung** und **Geräte** die erforderlichen Informationen ein. Wählen Sie den Bedingungstyp **Interne Ereignisübereinstimmung** aus, und klicken Sie dann auf die Registerkarte **Aktionen**.

   c Wählen Sie **Nachricht senden** aus, und klicken Sie dann auf **Konfigurieren**, um eine Vorlage für SNMP-Nachrichten auszuwählen oder zu erstellen.

   d Wählen Sie im Feld **SNMP** die Option **Standard-SNMP-Trap** aus, oder klicken Sie auf **Vorlagen** und dann auf **Hinzufügen**.

   e Wählen Sie eine vorhandene Vorlage aus, oder klicken Sie auf **Hinzufügen**, um eine neue Vorlage zu definieren.

   f Kehren Sie zur Seite **Alarmeinstellungen** zurück, und fahren Sie mit dem Einrichten des Alarms fort.

Hinzufügen eines Alarms zur Benachrichtigung bei Stromausfällen

Fügen Sie einen Alarm hinzu, damit Sie bei Ausfall einer der ESM-Stromversorgungen benachrichtigt werden.

Bevor Sie beginnen

Richten Sie einen SNMP-Trap für allgemeine Hardware-Fehler ein (siehe *Einrichten eines SNMP-Traps für Benachrichtigung bei Stromausfällen*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Alarme**, klicken Sie auf **Hinzufügen**, fügen Sie auf der Registerkarte **Übersicht** die erforderlichen Daten hinzu, und klicken Sie dann auf die Registerkarte **Bedingung**.

3 Wählen Sie im Feld **Typ** die Option **Interne Ereignisübereinstimmung** aus.

4 Wählen Sie im Feld **Feld** die Option **Signatur-ID** aus, und geben Sie dann `306-50086` in das Feld **Werte** ein.

5 Füllen Sie nach Bedarf die verbleibenden Informationen auf den einzelnen Registerkarten aus, und klicken Sie dann auf **Fertig stellen**.

Bei Ausfall einer Stromversorgung wird ein Alarm ausgelöst.

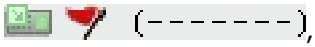
Hinzufügen eines Alarms für Integritätsüberwachungsereignisse

Durch Integritätsüberwachungsregeln werden Ereignisse generiert, die unter einem Basisgerät in der Systemnavigationsstruktur angezeigt werden.

Die Signatur-IDs der Integritätsüberwachungsereignisse können Sie im Feld **Werte** eines Alarms vom Typ **Interne Ereignisübereinstimmung** zum Generieren eines auf Integritätsüberwachungsereignissen basierenden Alarms verwenden. Der Bericht **Ereigniszusammenfassung für die Integritätsüberwachung** wird dann als Aktion des Alarms generiert.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

- Es gibt verschiedene Möglichkeiten, einen Alarm für Integritätsüberwachungsereignisse hinzuzufügen.

Einrichten eines Alarms	Vorgehensweise
Bevor ein Integritätsüberwachungsereignis generiert wird	1 Folgen Sie dem Prozess zum Erstellen eines Alarms (siehe *Erstellen eines Alarms*). 2 Klicken Sie in der Systemnavigationsstruktur auf **Bedingung**, und wählen Sie dann den Typ **Interne Ereignisübereinstimmung** aus. 3 Wählen Sie in der Zeile **Feld** die Option **Signatur-ID** aus. 4 Geben Sie im Feld **Werte** die Signatur-ID für die Integritätsüberwachungsregeln ein (siehe *Signatur-IDs für die Integritätsüberwachung*). 5 Geben Sie die verbleibenden Informationen gemäß der Beschreibung unter *Erstellen eines Alarms* ein.
Wenn bereits ein Integritätsüberwachungsereignis vorhanden ist	1 Klicken Sie in der Systemnavigationsstruktur auf das Basisgerät für das System  , und wählen Sie dann eine Ansicht aus, in der das Integritätsüberwachungsereignis angezeigt wird (**Ereignisanalyse** oder **Standardzusammenfassung**). 2 Klicken Sie auf das Ereignis und dann auf das Symbol **Menü**  . 3 Wählen Sie Folgendes aus: **Aktionen** | **Neuen Alarm erstellen von**aus, und klicken Sie dann auf **Signatur-ID**. 4 Füllen Sie die verbleibenden Einstellungen für den Alarm aus.

Siehe auch

Erstellen eines Alarms auf Seite 232

Signatur-IDs für die Integritätsüberwachung

Diese Liste enthält Beschreibungen der Integritätsüberwachungsregeln, die zugehörigen Signatur-IDs sowie Typ, Gerät und Schweregrad. Mit diesen Regeln können Sie einen Alarm erstellen, durch den

eine Benachrichtigung ausgelöst wird, wenn ein Ereignis im Zusammenhang mit einer Integritätsüberwachungsregel generiert wird.

Regelname	Signatur-ID	Beschreibung	Typ	Gerät	Schweregra
Eine Verbindung mit einer physischen Netzwerkschnittstelle wurde hergestellt oder entfernt.	306-50080	Einstellungen für Netzwerkschnittstellen wurden über eine SSH-Sitzung geändert.	Software-Monitor	ESM	Mittel
Es ist ein RAID-Fehler aufgetreten.	306-50054	Es sind RAID-Fehler aufgetreten.	Hardware-Monitor	Alle	Hoch
Das Konto wurde aufgrund von Inaktivität deaktiviert.	306-35	Das Benutzerkonto wurde aufgrund von Inaktivität deaktiviert.	Software-Monitor	ESM	Mittel
Das Konto wurde deaktiviert, da die maximale Anzahl für fehlgeschlagene Anmeldungen erreicht ist.	306-36	Das Benutzerkonto wurde deaktiviert, da die maximale Anzahl für fehlgeschlagene Anmeldungen erreicht ist.	Software-Monitor	ESM	Hoch
Hinzufügen oder Bearbeiten eines Remote-Befehls	306-60	Ein Alarm-Remote-Befehl wurde hinzugefügt oder gelöscht.	Software-Monitor	ESM	Niedrig
Warnung zur Statusänderung der erweiterten Syslog-Parser-Erfassung	306-50029	Der ASP-Parser wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
APM-Distiller-Prozess	306-50066	Das ADM-Textextrahierungsmodul für PDF/DOC wurde angehalten oder gestartet.	Software-Monitor	APM	Mittel
Eine nicht übereinstimmende Konfiguration wurde genehmigt.	146-7	Eine Änderung an einem Netzwerkerkennungsgerät wurde genehmigt.	Software-Monitor	ESM	Niedrig
Änderung der Archivkonfiguration	306-3	Die Archivierungseinstellungen für ESM wurden geändert.	Software-Monitor	ESM	Niedrig
Warnung zur Statusänderung des Archivprozesses	306-50051	Der Archivprozess des Empfängers wurde angehalten oder gestartet.	Software-Monitor	APM/REC/IPS/DBM	Mittel
Ereignis im Zusammenhang mit Ressourcenanfälligkeit	146-10, 306-10	Ein Schwachstellenereignis wurde erstellt.	Software-Monitor	ESM	Niedrig
Benutzeranmeldung des Audit-Administrators	306-38	UCAPL-Ereignis, Anmeldung des Audit-Administrators	Software-Monitor	ESM	Niedrig
Änderung der Sicherungskonfiguration	306-1	Die Konfigurationseinstellungen für die ESM-Sicherung wurden geändert.	Software-Monitor	ESM	Niedrig
Sicherung ausgeführt	306-2	Auf dem System wurde eine Sicherung ausgeführt.	Software-Monitor	ESM	Niedrig
Warnung zum Blue Martini-Parser	306-50071	Der Blue Martini-Parser wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zum Status der Umgehungs-Netzwerkkarte	306-50001	Die Netzwerkkarte hat den Umgehungsstatus angenommen oder verlassen.	Software-Monitor	IPA/ADM/IPS	Mittel
Das CAC-Zertifikat ist abgelaufen.	306-50082	Das CAC-Zertifikat für ESM ist abgelaufen.	Software-Monitor	ESM	Hoch
Das CAC-Zertifikat läuft bald ab.	306-50081	Das CAC-Zertifikat für ESM läuft bald ab.	Software-Monitor	ESM	Mittel
Der Fall wurde geändert.	306-70	Der Fall wurde geändert.	Software-Monitor	ESM	Niedrig

Regelname	Signatur-ID	Beschreibung	Typ	Gerät	Schweregra
Der Fallstatus wurde hinzugefügt, geändert oder gelöscht.	306-73	Der Fallstatus wurde geändert.	Software-Monitor	ESM	Niedrig
Warnung zur Statusänderung des Kommunikationskanals	306-50013	Der Steuerungskanal wurde angehalten oder gestartet.	Software-Monitor	Alle	Mittel
Die Aufzeichnung der Konfiguration ist fehlgeschlagen (Gerätefehler).	146-4	Gerätefehler bei der Netzwerkerkennung	Software-Monitor	ESM	Niedrig
Die Aufzeichnung der Konfiguration ist fehlgeschlagen (Gerät nicht erreichbar).	146-3	Das Gerät war bei der Netzwerkerkennung nicht erreichbar.	Software-Monitor	ESM	Niedrig
Die Konfiguration wurde aufgezeichnet.	146-5	Die Konfiguration der Netzwerkerkennung wurde erfolgreich überprüft.	Software-Monitor	ESM	Niedrig
Fehler bei einer Konfigurationsrichtlinie	146-8	Wird im System nicht verwendet.	Software-Monitor	ESM	Niedrig
Konfigurationsrichtlinie zulassen	146-9	Wird im System nicht verwendet.	Software-Monitor	ESM	Niedrig
Konfigurationsänderung für die Datenzuordnung	306-7	Die Einstellungen für die Datenzuordnung in ESM wurden geändert.	Software-Monitor	ESM	Hoch
Warnung zum freien Speicherplatz in der Datenpartition	306-50005	In den einzelnen Partitionen ist wenig freier Speicherplatz vorhanden (beispielsweise verfügt hada_hd über 10 % freien Speicherplatz).	Software-Monitor	Alle	Mittel
Konfigurationsänderung für die Datenaufbewahrung	306-6	Die Konfiguration für die Datenaufbewahrung in ESM wurde geändert.	Software-Monitor	ESM	Hoch
Warnung zum Status der Datenbank-Erkennungsdienste	306-50036	Der Dienst für die automatische DBM-Erkennung wurde angehalten oder gestartet.	Software-Monitor	Alle	Mittel
Warnung zur Statusänderung der gründlichen Paketprüfung	306-50008	Das Modul für die gründliche Paketprüfung in IPS oder ADM wurde angehalten oder gestartet.	Software-Monitor	Alle	Mittel
Der Remote-Befehl wurde gelöscht.	306-61	Der Alarm-Remote-Befehl wurde entfernt.	Software-Monitor	ESM	Niedrig
Ereignisse wurden gelöscht.	306-74	Der Benutzer hat ESM-Ereignisse gelöscht.	Software-Monitor	ESM	Niedrig
Flüsse wurden gelöscht.	306-75	Der Benutzer hat ESM-Flüsse gelöscht.	Software-Monitor	ESM	Niedrig
Hinzufügen eines Geräts	306-18	Ein neues Gerät wurde zum System hinzugefügt.	Software-Monitor	ESM	Niedrig
Löschen eines Geräts	306-19	Ein vorhandenes Gerät wurde aus dem System gelöscht.	Software-Monitor	ESM	Niedrig
Gerät möglicherweise inaktiv	146-2	Ereignis im Zusammenhang mit der Netzwerkerkennung, aus dem hervorgeht, dass ein Gerät möglicherweise inaktiv ist.	Software-Monitor	ESM	Niedrig
Das Gerät ist nicht erreichbar.	146-1	Das zu ESM hinzugefügte Netzwerkerkennungsgerät ist nicht erreichbar.	Software-Monitor	ESM	Niedrig

Regelname	Signatur-ID	Beschreibung	Typ	Gerät	Schweregra
Warnung zu Fehlern des Festplattenlaufwerks	306-50018	Überprüft die Integrität aller Festplattenlaufwerke (intern oder DAS).	Hardware-Monitor	Alle	Hoch
Warnung zur Statusänderung des ELM-Archivprozesses	306-50045	Das ELM-Komprimierungsmodul wurde angehalten oder gestartet.	Software-Monitor	APM/REC/IPS/DBM	Mittel
ELM-EDS-FTP	306-50074	Das ELM-SFTP-Programm wurde angehalten oder gestartet.	Software-Monitor	ELM	Mittel
ELM-Dateiprozess	306-50065	Das Modul für die erneute ELM-Einfügung wurde angehalten oder gestartet. Wenn bei einem Protokoll Fehler auftreten, wird die Einfügung erneut versucht. Wenn der Prozess der erneuten Einfügung fehlschlägt, wird diese Regel ausgelöst.	Software-Monitor	ELM	Mittel
ELM-FTI-Warnung	306-50064	Das Modul für die ELM-Volltextindizierung wurde angehalten oder gestartet.	Software-Monitor	ELM	Mittel
Warnung zur Statusänderung des ELM-Bereitstellungspunkts	306-50053	Der ELM-Remote-Speicher (CIFS, NFS, ISCSI, SAN) wurde angehalten oder gestartet.	Software-Monitor	ELM	Mittel
Warnung zur Statusänderung des ELM-Abfragemoduls	306-50046	Der ELM-Auftragsprozess (alle ELM-Aufträge wie unter anderem ELM-Abfragen und -Einfügungen) wurde angehalten oder gestartet.	Software-Monitor	ELM	Mittel
Redundanter ELM-Speicher	306-50063	Die ELM-Spiegelung wurde angehalten oder gestartet.	Software-Monitor	ELM	Mittel
Fehler in der ELM-Systemdatenbank	306-50044	Die ELM-Datenbank wurde angehalten oder gestartet.	Software-Monitor	ELM	Hoch
Warnung zur Statusänderung der E-Mail-Erfassung	306-50040	Die Cisco MARS-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
ePO-Tags wurden angewendet.	306-28	McAfee ePO-Tags wurden angewendet.	Software-Monitor	ESM	Niedrig
Fehler bei der Kommunikation mit ELM	306-50047	Die Kommunikation mit ELM ist fehlgeschlagen.	Software-Monitor	APM/REC/IPS/DBM	Hoch
Fehler bei der SSH Kommunikation	306-50077	Bei der Kommunikation mit ELM sind Geräteprobleme aufgetreten (beispielsweise unterschiedliche Versionen, geänderte Schlüssel).	Software-Monitor	Alle	Hoch
Neustart von ESM	306-32	ESM wurde neu gestartet.	Software-Monitor	ESM	Mittel
Herunterfahren von ESM	306-33	ESM wurde heruntergefahren.	Software-Monitor	ESM	Mittel
Warnung zur eStreamer-Erfassung	306-50070	Die eStreamer-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der eStreamer-Erfassung	306-50041	Die eStreamer-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Trennen der Ereignispartition	306-4	Die Ereignispartition wurde getrennt.	Software-Monitor	ESM	Niedrig

Regelname	Signatur-ID	Beschreibung	Typ	Gerät	Schweregra
Remote-Befehl ausführen	306-62	Der Alarm-Remote-Befehl wurde ausgeführt.	Software-Monitor	ESM	Niedrig
Die Anmeldung ist fehlgeschlagen, da die maximale Anzahl von gleichzeitigen Sitzungen erreicht war.	306-37	Die Anmeldung des Benutzers ist fehlgeschlagen, da die maximale Anzahl von gleichzeitigen Sitzungen erreicht war.	Software-Monitor	ESM	Hoch
Das Formatieren des SAN-Geräts ist fehlgeschlagen.	306-50057	Das Formatieren des SAN-Geräts in ELM ist fehlgeschlagen. Der Benutzer muss den Vorgang erneut versuchen.	Hardware-Monitor	ESM	Hoch
Die Benutzeranmeldung ist fehlgeschlagen.	306-31	Die Anmeldung des Benutzers ist fehlgeschlagen.	Software-Monitor	ESM	Mittel
Warnung zur Statusänderung der Dateierfassung	306-50049	Das Programm Mountcollector wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Die Datei wurde gelöscht.	306-50	Dies ist eine beliebige Datei, die hinzugefügt oder entfernt werden kann. Beispielsweise wurde eine Protokoll- oder Audiodatei von ESM entfernt.	Software-Monitor	ESM	Niedrig
Warnung zur Statusänderung der Filterverarbeitung	306-50050	Das Filterprogramm auf dem Gerät wurde angehalten oder gestartet (Filterregeln).	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der Firewall-Warnungsaggregation	306-50009	Die Firewall-Aggregation auf dem IPS- und/oder ADM-Gerät wurde angehalten oder gestartet.	Software-Monitor	IPS/ADM/ IPS	Mittel
Trennen der Flusspartition	306-5	Die Flusspartition wurde getrennt.	Software-Monitor	ESM	Niedrig
Fehler beim Abrufen der VA-Daten	306-52	Das Abrufen der VA-Daten durch ESM ist fehlgeschlagen.	Software-Monitor	ESM	Mittel
Erfolg beim Abrufen der VA-Daten	306-51	Die VA-Daten wurden von ESM abgerufen.	Software-Monitor	ESM	Niedrig
Interne Warnung zur Integritätsüberwachung	306-50027	Der Integritätsüberwachungsprozess wurde angehalten oder gestartet.	Software-Monitor	Alle	Mittel
Warnung zur Statusänderung der HTTP-Erfassung	306-50039	Die HTTP-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Änderung der Indizierungskonfiguration	306-8	Die Indizierungseinstellungen für ESM wurden geändert.	Software-Monitor	ESM	Mittel
Ungültiger SSH-Schlüssel	306-50075	Bei der Kommunikation mit ELM sind Geräteprobleme aufgetreten, beispielsweise unterschiedliche Versionen, geänderte Schlüssel.	Software-Monitor	Alle	Hoch
Warnung zur Statusänderung der IPFIX-Erfassung	306-50055	Die IPFIX-Erfassung (Fluss) wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Benutzeranmeldung des Schlüssel- und Zertifikat-Administrators	306-39	UCAPL-Ereignis, Anmeldung des Kryptografie-Administrators	Software-Monitor	ESM	Niedrig

Regelname	Signatur-ID	Beschreibung	Typ	Gerät	Schweregra
Die Protokollpartition wurde bereinigt.	306-34	Die ältesten Partitionen für die Protokolltabelle der Datenbank wurden bereinigt.	Software-Monitor	ESM	Niedrig
Warnung zum freien Speicherplatz in der Protokollpartition	306-50004	In der Protokollpartition (/var) ist wenig freier Speicherplatz vorhanden.	Software-Monitor	Alle	Mittel
Warnung zur Statusänderung des McAfee EDB-Datenbank-Servers	306-50010	Die Datenbank wurde angehalten oder gestartet.	Software-Monitor	Alle	Mittel
Warnung zur McAfee ePO-Erfassung	306-50069	Die McAfee ePO-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung des McAfee-Ereignisformats	306-50031	Die Erfassung des McAfee-Ereignisformats wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Kommunikationsfehler beim McAfee SIEM-Gerät	306-26	Die Kommunikation zwischen ESM und einem anderen Gerät ist nicht möglich.	Software-Monitor	ESM	Hoch
Warnung zu Microsoft Forefront Threat Management Gateway	306-50068	Die Forefront Threat Management Gateway-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung des MS-SQL-Abrufs	306-50035	Die MS SQL-Erfassung wurde angehalten oder gestartet (beliebige Datenquelle für MS SQL).	Software-Monitor	Empfänger	Mittel
Warnung zu einem Protokoll mit mehreren Ereignissen	306-50062	Die jEMAIL-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Der MVM-Scan wurde initiiert.	306-27	Der MVM-Scan wurde gestartet.	Software-Monitor	ESM	Niedrig
Warnung zur Statusänderung der NetFlow-Erfassung	306-50024	Die NetFlow-Erfassung (Fluss) wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Neues Benutzerkonto	306-13	Ein neuer Benutzer wurde zum System hinzugefügt.	Software-Monitor	ESM	Niedrig
Warnung zur Statusänderung der NFS-/CIFS-Erfassung	306-50048	Die Remote-Bereitstellung für NFS oder CIFS wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der NitroFlow-Erfassung	306-50026	NitroFlow (Flüsse auf dem Gerät) wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Es wurde kein SSH-Schlüssel gefunden.	306-50076	Bei der Kommunikation mit ELM sind Geräteprobleme aufgetreten, beispielsweise unterschiedliche Versionen, geänderte Schlüssel.	Software-Monitor	Alle	Hoch
Hinzufügen oder Ändern in der NSM-Blacklist	306-29	Ein NSM-Blacklist-Eintrag wurde hinzugefügt oder bearbeitet.	Software-Monitor	ESM	Niedrig
Löschen in der NSM-Blacklist	306-30	Ein NSM-Blacklist-Eintrag wurde gelöscht.	Software-Monitor	ESM	Niedrig
Warnung zur Statusänderung des OPSEC-Abrufs	306-50028	Die OPSEC-Erfassung (Check Point) wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel

Regelname	Signatur-ID	Beschreibung	Typ	Gerät	Schweregra
Warnung zur Statusänderung des OPSEC-Abrufs	306-50034	Die OPSEC-Erfassung (Check Point) wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Oracle IDM-Erfassung	306-50072	Die Oracle IDM-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Überbelegung	306-50012	ADM oder IPS hat den Überbelegungsmodus angenommen oder verlassen.	Software-Monitor	IPS/ADM/ IPS	Mittel
Warnung zum Erfassungs-/ Parser-Plug-In	306-50073	Das Erfassungs-/Parser-Plug-In wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Hinzufügen einer Richtlinie	306-15	Eine Richtlinie wurde zum System hinzugefügt.	Software-Monitor	ESM	Niedrig
Löschen einer Richtlinie	306-17	Eine Richtlinie wurde aus dem System gelöscht.	Software-Monitor	ESM	Niedrig
Ändern einer Richtlinie	306-16	Eine Richtlinie wurde im System geändert.	Software-Monitor	ESM	Niedrig
Keine Übereinstimmung mit der vorherigen Konfiguration	146-6	Die Konfiguration des Netzwerkerkennungsgeräts wurde geändert.	Software-Monitor	ESM	Niedrig
Empfänger-HA	306-50058	Ein HA-Prozess wurde angehalten oder gestartet (Corosync, HA-Steuerungsskript).	Software-Monitor	Empfänger	Mittel
OPSEC-Konfiguration für Empfänger-HA	306-50059	Wird nicht verwendet.	Software-Monitor	Empfänger	Niedrig
Das redundante ESM-Gerät ist nicht synchronisiert.	306-76	Das redundante ESM-Gerät ist nicht synchronisiert.	Software-Monitor	ESM	Hoch
Warnung zur Statusänderung von NFS-Remote-Bereitstellungspunkten	306-50020	Die NFS-ELM-Bereitstellung wurde angehalten oder gestartet.	Software-Monitor	ELM	Mittel
Warnung zum freien Speicherplatz von Remote-Freigaben/-Bereitstellungspunkten	306-50021	Auf dem Remote-Bereitstellungspunkt ist wenig freier Speicherplatz vorhanden.	Software-Monitor	ESM	Mittel
Warnung zur Statusänderung von SMB-/ CIFS-Remote-Freigaben	306-50019	Der SMB-/ CIFS-Remote-Bereitstellungspunkt wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der Risikokorrelation	306-50061	Das Risikokorrelationsmodul wurde angehalten oder gestartet.	Software-Monitor	ACE	Mittel
Warnung zum freien Speicherplatz in der Stammpartition	307-50002	In der Stammpartition ist wenig freier Speicherplatz vorhanden.	Software-Monitor	Alle	Mittel
Hinzufügen einer Regel	306-20	Eine Regel wurde zum System hinzugefügt, beispielsweise eine ASP-Regel, Filterregel oder Korrelationsregel.	Software-Monitor	ESM	Niedrig
Löschen einer Regel	306-22	Eine Regel wurde aus dem System gelöscht.	Software-Monitor	ESM	Niedrig

Regelname	Signatur-ID	Beschreibung	Typ	Gerät	Schweregra
Ändern einer Regel	306-21	Eine Regel wurde im System geändert.	Software-Monitor	ESM	Niedrig
Fehler bei der Regelaktualisierung	306-9	Die Regelaktualisierung für ESM ist fehlgeschlagen.	Software-Monitor	ESM	Mittel
Warnung zur Statusänderung des SDEE-Abrufs	306-50033	Die SDEE-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der sFlow-Erfassung	306-50025	Die sFlow-Erfassung (Fluss) wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der SNMP-Erfassung	306-50023	Die SNMP-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der SQL-Erfassung	306-50038	Die SQL-Erfassung (alt: NFX) wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der Symantec AV-Erfassung	306-50056	Die Symantec AV-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der Syslog-Erfassung	306-50037	Die Syslog-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Benutzeranmeldung des Systemadministrators	306-40	Der Systemadministrator hat sich beim System angemeldet.	Software-Monitor	ESM	Niedrig
Fehler bei der Überprüfung der Systemintegrität	306-50085	Ein auf dem System ausgeführtes fremdes Nicht-ISO-Programm oder ein entsprechender Prozess wird gekennzeichnet.	Software-Monitor	Alle	Hoch
Warnung zur Statusänderung der Systemprotokollierung	306-50014	Der Prozess der Systemprotokollierung wurde angehalten oder gestartet.	Software-Monitor	Alle	Mittel
Der Task (Abfrage) wurde beendet.	306-54	Der Task-Manager wurde geschlossen.	Software-Monitor	ESM	Niedrig
Warnung zum freien Speicherplatz in der temporären Partition	306-50003	In der temporären Partition (/tmp) ist wenig Speicherplatz vorhanden.	Software-Monitor	Alle	Mittel
Warnung zur Statusänderung des Textprotokoll-Parsers	306-50052	Der textparser-Prozess wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Änderung an Benutzerkonto	306-14	Das Benutzerkonto wurde geändert.	Software-Monitor	ESM	Niedrig
Fehler bei der Benutzeranmeldung beim Gerät	306-50079	Die Anmeldung des SSH-Benutzers ist fehlgeschlagen.	Software-Monitor	ESM	Niedrig
Benutzeranmeldung beim Gerät	306-50017	Wird im System nicht verwendet.	Software-Monitor	ESM	Niedrig
Benutzerabmeldung beim Gerät	306-50078	Der SSH-Benutzer hat sich abgemeldet.	Software-Monitor	ESM	Niedrig
Benutzeranmeldung	306-11	Der Benutzer hat sich beim System angemeldet.	Software-Monitor	ESM	Niedrig
Benutzerabmeldung	306-12	Der Benutzer hat sich beim System abgemeldet.	Software-Monitor	ESM	Niedrig
Warnung zum Status des VA-Datenmoduls	306-50043	Das VA-Modul (vaded.pl) wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel

Regelname	Signatur-ID	Beschreibung	Typ	Gerät	Schweregra
Hinzufügen einer Variablen	306-23	Eine Richtlinienvariable wurde hinzugefügt.	Software-Monitor	ESM	Niedrig
Löschen einer Variablen	306-25	Eine Richtlinienvariable wurde gelöscht.	Software-Monitor	ESM	Niedrig
Ändern einer Variablen	306-24	Eine Richtlinienvariable wurde geändert.	Software-Monitor	ESM	Niedrig
Das Web-Server-Zertifikat ist abgelaufen.	306-50084	Das ESM-Web-Server-Zertifikat ist abgelaufen.	Software-Monitor	ESM	Hoch
Das Web-Server-Zertifikat läuft bald ab.	306-50083	Das ESM-Web-Server-Zertifikat läuft bald ab.	Software-Monitor	ESM	Mittel
Warnung zur Websense-Erfassung	306-50067	Die Websense-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel
Warnung zur Statusänderung der Erfassung von WMI-Ereignisprotokollen	306-50030	Die WMI-Erfassung wurde angehalten oder gestartet.	Software-Monitor	Empfänger	Mittel

Kopieren eines Alarms

Sie können einen vorhandenen Alarm als Vorlage für einen neuen Alarm verwenden, indem Sie den Alarm kopieren und unter einem anderen Namen speichern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Alarme**.
2. Wählen Sie den zu kopierenden Alarm aus, und klicken Sie dann auf **Kopieren**.

   Auf der Seite **Alarmname** wird der Name des aktuellen Alarms gefolgt von `_copy` angezeigt.
3. Ändern Sie den Namen, und klicken Sie dann auf **OK**.
4. Zum Ändern der Alarmeinstellungen wählen Sie den kopierten Alarm aus, und klicken Sie auf **Bearbeiten**.
5. Ändern Sie die Einstellungen nach Bedarf.

Siehe auch

Erstellen eines Alarms auf Seite 232

Aktivieren oder Deaktivieren der Alarmüberwachung

Die Alarmüberwachung ist standardmäßig aktiviert. Sie können sie deaktivieren und dann bei Bedarf erneut aktivieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Alarme**.
2. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Deaktivieren**.

   Die Alarmüberwachung wird angehalten, und die Schaltfläche ändert sich in **Aktivieren**.
3. Klicken Sie auf **Aktivieren**, um die Überwachung der Alarme fortzusetzen.

Anpassen der Übersicht für ausgelöste Alarme und Fälle

Wählen Sie die Daten aus, die in der Alarmübersicht und in der Fallübersicht der Alarme vom Typ **Feldübereinstimmung** und **Interne Ereignisübereinstimmung** enthalten sein sollen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf der Seite **Systemeigenschaften** auf **Alarme** und dann auf **Hinzufügen**.
3. Wählen Sie auf der Registerkarte **Bedingung** den Typ **Feldübereinstimmung** oder **Interne Ereignisübereinstimmung** aus.
4. Klicken Sie auf die Registerkarte **Aktionen**, klicken Sie auf **Fall erstellen für** und dann auf das Variablensymbol  . Wählen Sie dann die Felder aus, die in der Fallübersicht enthalten sein sollen.
5. Klicken Sie auf **Übersicht für ausgelösten Alarm anpassen**, klicken Sie auf das Variablensymbol  , und wählen Sie dann die Felder aus, die in der Übersicht für den ausgelösten Alarm enthalten sein sollen.
6. Geben Sie die weiteren erforderlichen Informationen zum Einrichten des Alarms ein (siehe *Erstellen eines Alarms*), und klicken Sie dann auf **Fertig stellen**.

Verwalten von Nachrichtenvorlagen für Alarme

Eine der beim Einrichten eines Alarms verfügbaren Aktionen lautet **Nachricht senden**. Damit können Sie Alarminformationen an E-Mail-Empfänger oder ausgewählte SMS-Empfänger (Short Message Services), SNMP- oder Syslog-Empfänger weiterleiten. Sie können Vorlagen hinzufügen, um die in den Nachrichten enthaltenen Informationen zu definieren, und sie so gestalten, dass sie die für den Empfänger nützlichsten Informationen enthalten. Anschließend können Sie die Vorlage auswählen, wenn Sie die Aktion für einen Alarm definieren.

Sie können Vorlagen hinzufügen, um die in den Nachrichten enthaltenen Informationen zu definieren, und sie so gestalten, dass sie die für den Empfänger nützlichsten Informationen enthalten. Anschließend können Sie die Vorlage auswählen, wenn Sie die Aktion für einen Alarm definieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Alarme**.
2. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Vorlagen**.
3. Zeigen Sie die Liste der vorhandenen Vorlagen an, oder wählen Sie eine der verfügbaren Optionen aus. Klicken Sie dann auf **OK**.

Verwalten von Audiodateien für Alarme

Sie können Audiodateien hochladen und herunterladen, um sie für Audiowarnungen zu verwenden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Alarme**.
2. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Audio**.
3. Sie können Audiodateien herunterladen, hochladen, entfernen oder wiedergeben. Klicken Sie dann auf **Schließen**.

Verwalten von Alarmempfängern

Wenn Sie die Aktionseinstellungen für einen Alarm festlegen, können Sie eine Nachricht an Empfänger senden. Die Liste der Empfänger können Sie auf der Seite **Alarme** verwalten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Alarme**.
2. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Empfänger**.
3. Wählen Sie den Typ der zu verwaltenden Empfängerliste aus. Fügen Sie dann Empfänger hinzu, bearbeiten Sie sie, oder entfernen Sie sie.

Verwalten von Alarmen

Wenn ein Alarm ausgelöst wird, können Sie ihn bestätigen, löschen oder die Details anzeigen. Außerdem können Sie die Bestätigung eines Alarms aufheben, den Beauftragten ändern und aus einem Alarm einen Fall erstellen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Greifen Sie auf eines der folgenden Elemente zu:

- Protokollbereich **Alarm**: Befindet sich unter der Systemnavigationsstruktur.
- Visuelle Pop-Up-Warnung: Wird geöffnet, wenn ein Alarm ausgelöst wird.
- Seite **Details**: Wird geöffnet, wenn Sie auf das Symbol **Details**  im Protokollbereich **Alarme** klicken.

2 Führen Sie einen oder mehrere der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Bestätigen eines Alarms	Klicken Sie auf das Symbol **Bestätigen**  .
Aufheben der Bestätigung eines Alarms	Klicken Sie auf das Symbol **Bestätigung aufgehoben**  .
Löschen eines Alarms	Klicken Sie auf das Symbol **Löschen**  .
Anzeigen von Alarmdetails	Klicken Sie im Protokollbereich **Alarme** oder in einer visuellen Pop-Up-Warnung auf das Symbol **Details**  .
Ändern des Beauftragten	Klicken Sie auf der Seite **Details** auf **Beauftragter**, und wählen Sie einen Namen aus.
Erstellen eines Falls aus einem Alarm	Klicken Sie auf der Seite **Details** auf **Fall erstellen**.

Aufgaben

- *Anzeigen der Warteschlange für Alarmberichte* auf Seite 250
  Wenn Sie für einen Alarm die Aktion **Berichte generieren** ausgewählt haben, können Sie Änderungen an den auf die Ausführung wartenden Berichten vornehmen und die abgeschlossenen Berichte anzeigen.
- *Verwalten von Alarmberichtsdateien* auf Seite 251
  Wenn ein Alarmbericht ausgeführt wurde, wird er der Liste der verfügbaren Berichte in ESM hinzugefügt. Sie können diese Liste anzeigen und verschiedene Aktionen ausführen.

Siehe auch

Hinzufügen eines Falls auf Seite 311

Anzeigen der Warteschlange für Alarmberichte

Wenn Sie für einen Alarm die Aktion **Berichte generieren** ausgewählt haben, können Sie Änderungen an den auf die Ausführung wartenden Berichten vornehmen und die abgeschlossenen Berichte anzeigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, klicken Sie auf **Alarme** und dann auf die Registerkarte **Einstellungen**.
2. Führen Sie einen der folgenden Schritte aus:
   - Zum Anzeigen oder Abbrechen von Berichten in der Ausführungswarteschlange klicken Sie auf **Ansicht**.
   - Zum Anzeigen und Verwalten abgeschlossener Berichte klicken Sie auf **Dateien**.
3. Klicken Sie auf **Schließen**.

Verwalten von Alarmberichtsdateien

Wenn ein Alarmbericht ausgeführt wurde, wird er der Liste der verfügbaren Berichte in ESM hinzugefügt. Sie können diese Liste anzeigen und verschiedene Aktionen ausführen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Alarme**.
2. Klicken Sie auf die Registerkarte **Einstellungen**, klicken Sie auf **Dateien**, und wählen Sie dann aus, ob Berichte aus der Liste heruntergeladen oder entfernt werden sollen oder ob Berichte in die Liste hochgeladen werden sollen.
3. Klicken Sie auf **Schließen**.

7 Arbeiten mit Ereignissen

Sie können mit ESM Milliarden von Ereignissen und Flüssen identifizieren, erfassen, verarbeiten, korrelieren und speichern. Dabei stehen alle Informationen für Abfragen, forensische Funktionen, Überprüfung von Regeln und Compliance zur Verfügung.

Inhalt

- *Ereignisse, Flüsse und Protokolle*
- *Verwalten von Berichten*
- *Beschreibung der contains-Filter und Filter für reguläre Ausdrücke*
- *Arbeiten mit ESM-Ansichten*
- *Benutzerdefinierte Typfilter*

Ereignisse, Flüsse und Protokolle

In *Ereignissen*, *Flüssen* und *Protokollen* werden unterschiedliche Arten von Aktivitäten aufgezeichnet, die auf einem Gerät auftreten.

Ein *Ereignis* ist eine Aktivität, die als Ergebnis einer im System vorhandenen Regel von einem Gerät aufgezeichnet wurde. Ein *Fluss* ist ein Datensatz für eine zwischen IP-Adressen hergestellte Verbindung, bei denen sich mindestens eine der IP-Adressen in Ihrem Heimnetzwerk (HOME_NET) befindet. Ein *Protokoll* ist ein Datensatz für ein Ereignis, das auf einem Gerät im System aufgetreten ist. Ereignisse und Flüsse haben Quell- und Ziel-IP-Adressen, Quell- und Ziel-Ports, Quell- und Ziel-MAC-Adressen (Media Access Control), ein Protokoll sowie eine Angabe für Erstes Mal und Letztes Mal (als Hinweis auf den Zeitraum zwischen Initiierung und Trennung der Verbindung). Es gibt jedoch mehrere Unterschiede zwischen Ereignissen und Flüssen:

- Da Flüsse keinen Hinweis auf anomalen oder bösartigen Datenverkehr darstellen, sind sie häufiger anzutreffen als Ereignisse.
- Im Gegensatz zu einem Ereignis ist ein Fluss nicht einer Regelsignatur (Signatur-ID) zugeordnet.
- Flüsse sind nicht Ereignisaktionen wie Warnung, Verwerfen und Ablehnen zugeordnet.
- Bestimmte Daten beziehen sich eindeutig auf Flüsse. Dazu gehören Quell- und Ziel-Bytes sowie Quell- und Zielpakete. Bei *Quell-Bytes und Quellpaketen* handelt es sich um die Anzahl der Bytes und Pakete, die von der Quelle des Flusses übermittelt wurden, während die *Ziel-Bytes und Zielpakete* die Anzahl der Bytes und Pakete darstellen, die vom Ziel des Flusses übermittelt wurden.
- Flüsse haben eine Richtung: Ein *eingehender Fluss* ist definiert als ein Fluss, dessen Ursprung sich außerhalb des Heimnetzwerks (HOME_NET) befindet. Ein *ausgehender Fluss* hat seinen Ursprung außerhalb des Heimnetzwerks (HOME_NET). Diese Variable wird in einer Richtlinie für ein Nitro IPS-Gerät definiert.

Die vom System generierten Ereignisse und Flüsse können Sie in Ansichten anzeigen, die Sie in der Dropdown-Liste für Ansichten auswählen. Protokolle werden unter den Optionen **Systemprotokoll** oder **Geräteprotokoll** aufgeführt, auf die Sie über die Seite **Eigenschaften** für das System oder das jeweilige Gerät zugreifen.

Einrichten von Downloads für Ereignisse, Flüsse und Protokolle

Überprüfen Sie manuell, ob Ereignisse, Flüsse und Protokolle vorhanden sind, oder legen Sie fest, dass diese Überprüfung automatisch vom Gerät ausgeführt wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Ereignisse, Flüsse und Protokolle**, **Ereignisse und Protokolle** oder **Protokolle**.

3 Richten Sie die Downloads ein, und klicken Sie dann auf **Anwenden**.

Begrenzen der Erfassungszeit für Daten

Sie können durch Planen eines täglichen Zeitbereichs begrenzen, wann vom ESM-Gerät die Daten von den einzelnen Geräten abgerufen werden und wann die Daten von den einzelnen Geräten an das ELM-Gerät gesendet werden.

> **Bevor Sie beginnen**
> Deaktivieren Sie die **Dynamische Aggregation**, und legen Sie **Aggregationsebene 1** auf einen Wert zwischen 240 und 360 Minuten fest (siehe *Ändern von Einstellungen für die Ereignis- oder Flussaggregation*).

Mit dieser Funktion können Sie vermeiden, dass das Netzwerk zu Spitzenzeiten verwendet wird, sodass die Bandbreite anderen Anwendungen zur Verfügung steht. Da dadurch die Zustellung der Daten an ESM und ELM verzögert wird, müssen Sie entscheiden, ob diese Verzögerung in der jeweiligen Umgebung akzeptabel ist.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.



Seien Sie vorsichtig, wenn Sie diese Funktion konfigurieren, da das Planen der Erfassung von Ereignissen, Flüssen und Protokollen zu Datenverlusten führen kann.

1 Wählen Sie in der Systemnavigationsstruktur das Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Wählen Sie eine der folgenden Optionen aus:

- **Ereignisse, Flüsse und Protokolle**
- **Ereignisse und Protokolle**
- **Protokolle**

3 Wählen Sie **Definieren Sie einen Zeitbereich für den täglichen Datenabruf** aus, und legen Sie dann Start- und Endzeit des Zeitbereichs fest.

Die Daten des Geräts werden auf dem ESM-Gerät erfasst und an das ELM-Gerät gesendet, damit sie dort im definierten Zeitbereich protokolliert werden. Wenn Sie dies auf einem ELM-Gerät einrichten,

definieren Sie damit, wann Daten vom ELM-Gerät auf dem ESM-Gerät erfasst werden und wann Daten vom ESM-Gerät zur Protokollierung an das ELM-Gerät gesendet werden.

Definieren der Einstellungen für den Schwellenwert für Inaktivität

Wenn Sie einen Schwellenwert für Inaktivität für ein Gerät festlegen und im angegebenen Zeitraum keine Ereignisse oder Flüsse generiert werden, werden Sie benachrichtigt. Wenn der Schwellenwert erreicht ist, wird in der Systemnavigationsstruktur neben dem Geräteknoten eine gelbe Kennzeichnung für den Integritätsstatus angezeigt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, stellen Sie sicher dass **Systeminformationen** ausgewählt ist, und klicken Sie dann auf **Ereignisse, Flüsse und Protokolle**.
2. Klicken Sie auf **Einstellungen für Inaktivität**.
3. Geben Sie das Gerät hervor, und klicken Sie dann auf **Bearbeiten**.
4. Nehmen Sie Änderungen an den Einstellungen vor, und klicken Sie dann auf **OK**.

Abrufen von Ereignissen und Flüssen

Rufen Sie Ereignisse und Flüsse für die in der Systemnavigationsstruktur ausgewählten Geräte ab.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System, eine Gruppe oder ein Gerät aus.
2. Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Ereignisse und Flüsse abrufen**  , und führen Sie dann die erforderlichen Schritte aus.
3. Wählen Sie nach Abschluss des Downloads eine Ansicht aus, in der die Ereignisse und Flüsse angezeigt werden sollen. Klicken Sie dann auf der Ansichtssymbolleiste auf das Symbol **Aktuelle Ansicht aktualisieren**  .

Überprüfen auf Ereignisse, Flüsse und Protokolle

Sie können festlegen, dass die Überprüfung auf Ereignisse, Flüsse und Protokolle vom ESM-Gerät automatisch ausgeführt wird, oder Sie können die Überprüfung manuell ausführen. Die Häufigkeit der Überprüfung hängt vom Ausmaß der Aktivitäten in Ihrem System ab und davon, wie oft Sie Statusaktualisierungen erhalten möchten. Sie können auch festlegen, auf welchen Geräten welche Informationsarten überprüft werden sollen, und die Einstellungen für den Schwellenwert für Inaktivität für die vom ESM-Gerät verwalteten Geräte festlegen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Ereignisse, Flüsse und Protokolle**.
2. Wählen Sie die entsprechenden Optionen für den Abruf von Ereignissen, Flüssen und Protokollen aus, und nehmen Sie gegebenenfalls Änderungen vor.
3. Klicken Sie auf **OK**.

Siehe auch

Definieren der Einstellungen für den Schwellenwert für Inaktivität auf Seite 255

Definieren von Geolocation- und ASN-Einstellungen

Über *Geolocation* erhalten Sie den tatsächlichen geografischen Standort von mit dem Internet verbundenen Computern. *ASN (Autonomous System Number)* ist eine Zahl, die einem autonomen System zugewiesen wird und jedes Netzwerk im Internet eindeutig identifiziert.

Mithilfe dieser beiden Datentypen können Sie den physischen Standort einer Bedrohung identifizieren. Daten für Quell- und Ziel-Geolocation können für Ereignisse erfasst werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Ereignisse, Flüsse und Protokolle** oder **Ereignisse und Protokolle** und dann auf **Geolocation**.
3. Wählen Sie die entsprechenden Optionen zum Generieren der gewünschten Informationen aus, und klicken Sie dann auf **OK**.

Anhand dieser Informationen können Sie Ereignisdaten filtern.

Abrufen von Ereignissen und Flüssen

Rufen Sie Ereignisse und Flüsse für die in der Systemnavigationsstruktur ausgewählten Geräte ab.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System, eine Gruppe oder ein Gerät aus.
2. Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Ereignisse und Flüsse abrufen**  , und führen Sie dann die erforderlichen Schritte aus.
3. Wählen Sie nach Abschluss des Downloads eine Ansicht aus, in der die Ereignisse und Flüsse angezeigt werden sollen. Klicken Sie dann auf der Ansichtssymbolleiste auf das Symbol **Aktuelle Ansicht aktualisieren**  .

Aggregieren von Ereignissen oder Flüssen

Ein Ereignis oder Fluss kann theoretisch tausendfach generiert werden. Sie müssen nicht Tausende identischer Ereignisse durchgehen, sondern können mithilfe der Aggregation diese Ereignisse als ein

einziges Ereignis bzw. einen einzigen Fluss anzeigen. Dabei gibt ein Zähler an, wie oft ein Ereignis aufgetreten ist.

Bei der Aggregation wird der Speicherplatz sowohl auf dem Gerät als auch in ESM effizienter genutzt, da nicht jedes einzelne Paket gespeichert werden muss. Diese Funktion gilt nur für Regeln, für die im **Richtlinien-Editor** die Aggregation aktiviert ist.

Quell-IP-Adresse und Ziel-IP-Adresse

Die "nicht festgelegten" Werte oder aggregierten Werte für Quell-IP-Adresse und Ziel-IP-Adresse werden in allen Ergebnissätzen als "::" anstelle von "0.0.0.0" angezeigt. Beispiel:

- `::ffff:10.0.12.7` wird als `0:0:0:0:0:FFFF:A00:C07` eingefügt (`A00:C07` entspricht `10.0.12.7`).
- `::0000:10.0.12.7` entspricht `10.0.12.7`.

Aggregierte Ereignisse und Flüsse

In aggregierten Ereignissen und Flüssen wird mit den Feldern Erstes Mal, Letztes Mal und Insgesamt die Dauer und Menge der Aggregation angegeben. Beispiel: Ein Ereignis ist in den ersten zehn Minuten nach 12:00 Uhr 30 Mal aufgetreten. Das Feld **Erstes Mal** enthält die Uhrzeit 12:00 Uhr (den Zeitpunkt der ersten Instanz des Ereignisses), das Feld **Letztes Mal** enthält die Uhrzeit 12:10 Uhr (den Zeitpunkt der letzten Instanz des Ereignisses), und das Feld **Insgesamt** enthält den Wert 30.

Sie können die Standardeinstellungen für Ereignisse oder die Flussaggregation für das Gerät insgesamt ändern und für einzelne Regeln Ausnahmen für die Einstellungen des Geräts hinzufügen (siehe *Verwalten von Aggregationsausnahmen für Ereignisse*).

Die dynamische Aggregation ist auch standardmäßig aktiviert. Wenn sie ausgewählt ist, werden die Einstellungen für **Aggregationsebene 1** ersetzt und die Einstellungen für **Aggregationsebene 2** und **Aggregationsebene 3** erhöht. Datensätze werden basierend auf der Abrufeinstellung für Ereignisse, Flüsse und Protokolle abgerufen. Wenn automatisches Abrufen festgelegt ist, wird ein Datensatz nur beim ersten Abruf durch ESM vom Gerät komprimiert. Wenn manuelles Abrufen festgelegt ist, wird ein Datensatz bis zu 24 Stunden lang komprimiert oder bis zum manuellen Abruf eines neuen Datensatzes, je nachdem, was zuerst geschieht. Wenn das 24-Stunden-Limit für die Komprimierung erreicht ist, wird ein neuer Datensatz abgerufen, und die Komprimierung beginnt für diesen neuen Datensatz.

Ändern von Einstellungen für die Ereignis- oder Flussaggregation

Ereignisaggregation und Flussaggregation sind standardmäßig aktiviert und auf **Hoch** festgelegt. Sie können die Einstellungen nach Bedarf ändern. Die Auswirkungen der einzelnen Einstellungen werden auf der Seite **Aggregation** beschrieben.

Bevor Sie beginnen

Zum Ändern dieser Einstellungen benötigen Sie die Berechtigungen **Richtlinienadministrator** und **Geräteverwaltung** oder **Richtlinienadministrator** und **Benutzerdefinierte Regeln**.



Die Ereignisaggregation ist nur für ADM- und IPS-Geräte sowie Empfängergeräte verfügbar, die Flussaggregation ist für IPS-Geräte und Empfängergeräte verfügbar.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Ereignisaggregation** oder **Flussaggregation**.
3. Definieren Sie die Einstellungen, und klicken Sie dann auf **OK**.

Hinzufügen von Ausnahmen für Einstellungen für die Ereignisaggregation

Aggregationseinstellungen gelten für alle von einem Gerät generierten Ereignisse. Sie können Ausnahmen für einzelne Regeln erstellen, wenn die allgemeinen Einstellungen für die von der jeweiligen Regel generierten Ereignisse nicht gelten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie im Ansichtsbereich ein Ereignis aus, das von der Regel generiert wurde, für die Sie eine Ausnahme hinzufügen möchten.
2. Klicken Sie auf das Symbol **Menü**  , und wählen Sie dann **Aggregationseinstellungen ändern** aus.
3. Wählen Sie in den Dropdown-Listen **Feld 2** und **Feld 3** die zu aggregierenden Feldtypen aus.



Sie müssen in **Feld 2** und **Feld 3** unterschiedliche Typen auswählen, da ansonsten ein Fehler auftritt. Wenn Sie diese Feldtypen auswählen, werden die Beschreibungen der einzelnen Aggregationsebenen geändert und spiegeln nun die ausgewählten Optionen wider. Die Zeitlimits für die einzelnen Ebenen hängen von der für das Gerät definierten Einstellung für die Ereignisaggregation ab.

4. Klicken Sie auf **OK**, um die Einstellungen zu speichern und dann auf **Ja**, um fortzufahren.
5. Heben Sie die Auswahl von Geräten auf, für die Sie keinen Rollout der Änderungen ausführen möchten.
6. Klicken Sie auf **OK**, um den Rollout für die Änderungen auf den ausgewählten Geräten auszuführen.

In der Spalte **Status** wird beim Rollout der Änderungen der Aktualisierungsstatus angezeigt.

Verwalten von Aggregationsausnahmen für Ereignisse

Sie können eine Liste der Aggregationsausnahmen für Ereignisse anzeigen, die zum System hinzugefügt wurden. Außerdem können Sie eine Ausnahme bearbeiten oder entfernen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Ereignisaggregation** und dann unten auf dem Bildschirm auf **Ansicht**.
3. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf **Schließen**.

Einrichten der Ereignisweiterleitung

Mithilfe der Ereignisweiterleitung können Sie über Syslog oder SNMP (falls aktiviert) Ereignisse vom ESM-Gerät an ein anderes Gerät oder eine andere Einrichtung senden. Sie müssen das Ziel definieren und können auswählen, ob Sie das Paket einschließen und die IP-Daten verschleiern möchten. Sie können Filter hinzufügen, damit die Ereignisdaten vor der Weiterleitung gefiltert werden.

Diese Funktion ist kein Ersatz für die Protokollverwaltung, da es sich nicht um einen vollständigen Satz digital signierter Protokolle von den einzelnen Geräten in der Umgebung handelt.

Konfigurieren der Ereignisweiterleitung

Sie können ein Ereignisweiterleitungsziel einrichten, um Ereignisdaten an einen Syslog- oder SNMP-Server weiterzuleiten.

Die Anzahl der verwendeten Ereignisweiterleitungsziele in Kombination mit der Rate und Anzahl der vom ESM-Gerät abgerufenen Ereignisse kann sich auf die allgemeine ESM-Leistung auswirken.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Ereignisweiterleitung**.
2. Wählen Sie auf der Seite **Ereignisweiterleitungsziele** die Option **Hinzufügen**, **Bearbeiten** oder **Entfernen** aus.
3. Wenn Sie das Hinzufügen oder Bearbeiten eines Ziels ausgewählt haben, definieren Sie die Einstellungen.
4. Klicken Sie auf **Anwenden** oder **OK**.

Hinzufügen von Ereignisweiterleitungszielen

Fügen Sie ein Ereignisweiterleitungsziel zum ESM-Gerät hinzu, um Ereignisdaten an einen Syslog- oder SNMP-Server weiterzuleiten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Ereignisweiterleitung**.
2. Klicken Sie auf **Hinzufügen**, und geben Sie dann die erforderlichen Informationen ein.
3. Klicken Sie auf **OK**.

Siehe auch

Ereignisweiterleitungs-Agenten auf Seite 260

Ereignisweiterleitungs-Agenten

In der folgenden Tabelle finden Sie die Ereignisweiterleitungs-Agenten und die Informationen, die in den weitergeleiteten Paketen enthalten sind. Sie wählen den Agenten auf der Seite **Ereignisweiterleitungsziel hinzufügen** im Feld **Format** aus.

Agent	Inhalt
Syslog (McAfee 9.2)	ESM IP McAfee ESM (Bestandteil des Syslog-Headers), Signatur-ID (SigID), Signaturnachricht (SigMessage), Quell-IP (SrcIP), (Ziel-IP) DstIP, Quellport (SrcPort), Zielport (DstPort), Quell-MAC (SrcMac), Ziel-MAC (DstMac), Protokoll, VLAN, Fluss (gibt an, ob das Ereignis vom Initiator oder Empfänger der Verbindung generiert wird), Ereignisanzahl (EventCount), Erstes Mal (FirstTime) (im UNIX-Zeitformat), Letztes Mal (LastTime) (im UNIX-Zeitformat), Letztes Mal_Mikrosekunden (LastTime_usec), Ergebnisuntertyp, Schweregrad, Interne ID (InternalID) (Ereignis-ID auf dem ESM-Gerät), Ereignis-ID (EventID), IPS-ID (IPSID), IPS-Name (IPSName) (Name der Datenquelle: IP-Adresse), Datenquellen-ID (DSID), Quell-IPv6, Ziel-IPv6, Sitzungs-ID, Sequenz, Als vertrauenswürdig gekennzeichnet, Normalisierte ID, GUID-Quelle, GUID-Ziel, Agg 1 Name, Agg 1 Wert, Agg 2 Name, Agg 2 Wert, Agg 3 Name, Agg 3 Wert. Die folgenden Zeichenfolgenfelder sind außerdem in Anführungszeichen eingeschlossen, da sie ein Semikolon enthalten können: Application, Command, Domain, Host, Object, Destination User, Source User, User-defined type 8, User-defined type 9, User-defined type 10, User-defined type 21, User-defined type 22, User-defined type 23, User-defined type 24, User-defined type 25, User-defined type 26, User-defined type 27. Packet (Paketinhalt ist nur mit Base 64 codiert, wenn die Option "Paket kopieren" für die Regeln im Richtlinien-Editor auf "An" festgelegt ist und die Option beim Einrichten der Ereignisweiterleitung auf dem ESM-Gerät aktiviert wird).
Syslog (McAfee 8.2)	ESM IP McAfee ESM (Bestandteil des Syslog-Headers), Signatur-ID (SigID), Signaturnachricht (SigMessage), Quell-IP (SrcIP), (Ziel-IP) DstIP, Quellport (SrcPort), Zielport (DstPort), Quell-MAC (SrcMac), Ziel-MAC (DstMac), Protokoll, VLAN, Fluss (gibt an, ob das Ereignis vom Initiator oder Empfänger der Verbindung generiert wird), Ereignisanzahl (EventCount), Erstes Mal (FirstTime) (im UNIX-Zeitformat), Letztes Mal (LastTime) (im UNIX-Zeitformat), Letztes Mal_Mikrosekunden (LastTime_usec), Ergebnisuntertyp, Schweregrad, Interne ID (InternalID) (Ereignis-ID auf dem ESM-Gerät), Ereignis-ID (EventID), IPS-ID (IPSID), IPS-Name (IPSName) (Name der Datenquelle: IP-Adresse), Datenquellen-ID (DSID), Quell-IPv6, Ziel-IPv6, Sitzungs-ID, Sequenz, Als vertrauenswürdig gekennzeichnet, Normalisierte ID. Die folgenden Zeichenfolgenfelder sind außerdem in Anführungszeichen eingeschlossen, da sie ein Semikolon enthalten können: Application, Command, Domain, Host, Object, Destination User, Source User, User-defined type 8, User-defined type 9, User-defined type 10. Packet (Paketinhalt ist nur mit Base 64 codiert, wenn die Option "Paket kopieren" für die Regeln im Richtlinien-Editor auf "An" festgelegt ist und die Option beim Einrichten der Ereignisweiterleitung auf dem ESM-Gerät aktiviert wird).
Syslog (Nitro)	ESM IP, "McAfee ESM," Signatur-ID (SigID), Signaturnachricht (SigMessage), Quell-IP (SrcIP), (Ziel-IP) DstIP, Quellport (SrcPort), Zielport (DstPort), Quell-MAC (SrcMac), Ziel-MAC (DstMac), Protokoll, VLAN, Fluss (gibt an, ob das Ereignis vom Initiator oder Empfänger der Verbindung generiert wird), Ereignisanzahl (EventCount), Erstes Mal (FirstTime) (im UNIX-Zeitformat), Letztes Mal (LastTime) (im UNIX-Zeitformat), Letztes Mal_Mikrosekunden (LastTime_usec), Ergebnisuntertyp, Schweregrad, Interne ID (InternalID) (Ereignis-ID auf dem ESM-Gerät), Ereignis-ID (EventID), IPS-ID (IPSID), IPS-Name (IPSName), Datenquellen-ID (DSID), Paket (Paketinhalt ist mit Base 64 codiert).
Syslog (ArcSight)	"McAfee," MachineID, "ArcSite Notification," "Line 1," Gruppenname, IPS-Name, Letztes Mal (LastTime) mm/dd/yyy HH:nn:ss.zzz, Letztes Mal Mikrosekunden (LastTime usec), Erstes Mal (FirstTime) mm/dd/yyy HH:nn:ss.zzz, Signatur-ID (SigID), Klassenname (Class Name), Ereignisanzahl (Event Count), Quell-IP (Src IP), Quellport (Src Port), Ziel-IP (Dst IP), Zielport (Dst Port), Protokoll, Ereignisuntertyp, Ereignis-ID des Geräts (interne ID für das Ereignis vom Gerät), Ereignis-ID für ESM (interne ID für das Ereignis vom ESM-Gerät), Regelnachricht, Fluss (gibt an, ob das Ereignis vom Initiator oder Empfänger der Verbindung generiert wird), VLAN, Quell-MAC, Ziel-MAC, Paket (Paketinhalt ist mit Base 64 codiert).

Agent	Inhalt
Syslog (Snort)	snort:, [sigid:smallsigid:0], Signature Message oder "Alert", [Classification: ClassName], [Priority: ClassPriority], {Protocol}, SrcIP:SrcPort -> DstIP:DstPort, SrcIP -> DstIP, Packet (Paketinhalt ist mit Base 64 codiert).
Syslog (Audit-Protokolle)	time (Sekunden seit Epoche), status flag, user name, log category name (leer für 8.2.0, ausgefüllt für 8.3.0+), device group name, device name, log message.
Syslog (Einheitliches Ereignisformat)	Aktuelles Datum und aktuelle Uhrzeit, ESM-IP, CEF-Version 0, vendor = McAfee, product = ESM-Modell aus /etc/McAfee Nitro/ipsmodel, version = ESM-Version aus /etc/buildstamp, sig id, sig message, severity (0 bis 10), Paare aus Name und Wert, deviceTranslatedAddress
Syslog (Standardereignisformat)	<#>YYYY-MM-DDTHH:MM:SS.S [IP Address] McAfee_SIEM: { "source": { "id": 144120685667549200, "name": "McAfee Email Gateway (ASP)", "subnet": "::ffff:10.75.126.2/128" }, "fields": { "packet": { "encoding": "BASE64" } }, "data": { "unique_id": 1, "alert_id": 1, "thirdpartytype": 49, "sig": { "id": 5000012, "name": "Random String Custom Type" }, "norm_sig": { "id": 1343225856, "name": "Misc Application Event" }, "action": "5", "src_ip": "65.254.48.200", "dst_ip": "0.0.0.0", "src_port": 38129, "dst_port": 0, "protocol": "n/a", "src_mac": "00:00:00:00:00:00", "dst_mac": "00:00:00:00:00:00", "src_asn_geo": 1423146310554370000, "firsttime": "2014-05-09T20:43:30Z", "lasttime": "2014-05-09T20:43:30Z", "writetime": "2014-05-09T20:44:01Z", "src_guid": "", "dst_guid": "", "total_severity": 25, "severity": 25, "eventcount": 1, "flow": "0", "vlan": "0", "sequence": 0, "trusted": 2, "session_id": 0, "compression_level": 10, "reviewed": 0, "a1_ran_string_CF1": "This is data for custom field 1", "packet": "PDE0PjA5MDUyMDE0IDIwOjE4OjQ0fDIxfDY1LjI1NC40OC4yMDAtMzgxMjl8MXwxMDJ8U3BhbSBNZXNzYWdlIHR5cGU6IFRydXN0ZWRTb3VyY2UgU2lnbmF0dXJlIENvbmZpZGVuY2UgPSBISUdILiBDb25uZWN0aW9uOiA2NS4yNTQuNDguMjAwLTM4MTI5KElQLVBvcnQpfFRoaXMgaXMgZGF0YSBm b3IgY3VzdG9tIGZpZWxkIDF8W10A"

Aktivieren oder Deaktivieren der Ereignisweiterleitung

Aktivieren oder deaktivieren Sie die Ereignisweiterleitung auf dem ESM-Gerät.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Ereignisweiterleitung**.
2. Klicken Sie auf **Einstellungen**, und wählen Sie dann **Ereignisweiterleitung aktiviert** aus, oder heben Sie die Auswahl dieser Option auf.
3. Klicken Sie auf **OK**.

Ändern von Einstellungen für alle Ereignisweiterleitungsziele

Ändern Sie Einstellungen für alle vorhandenen Ereignisweiterleitungsziele gleichzeitig.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Ereignisweiterleitung**.
2. Klicken Sie auf **Einstellungen**, und legen Sie dann die Optionen fest.
3. Klicken Sie auf **OK**.

Hinzufügen von Ereignisweiterleitungsfiltern

Richten Sie Filter ein, um die Ereignisdaten zu begrenzen, die an einen Syslog- oder SNMP-Server auf dem ESM weitergeleitet werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Ereignisweiterleitung**.
2. Klicken Sie auf **Hinzufügen** und dann auf **Ereignisfilter**.
3. Füllen Sie die Filterfelder aus, und klicken Sie dann auf **OK**.

Bearbeiten von Einstellungen für Ereignisweiterleitungsfilter

Ändern Sie gespeicherte Filtereinstellungen für die Ereignisweiterleitung.

> **Bevor Sie beginnen**
>
> Wenn Sie einen Gerätefilter bearbeiten, benötigen Sie Zugriff auf alle Geräte im Filter. Informationen zum Aktivieren des Zugriffs auf die Geräte finden Sie unter *Einrichten von Benutzergruppen*.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Ereignisweiterleitung**.
2. Klicken Sie auf **Bearbeiten** und dann auf **Ereignisfilter**.
3. Nehmen Sie die Änderungen vor, und klicken Sie dann auf **OK**.

Siehe auch

Einrichten von Benutzergruppen auf Seite 206

Senden und Weiterleiten von Ereignissen mit Standardereignisformat

Das Standardereignisformat (Standard Event Format, SEF) ist ein JSON-basiertes (Java Script Object Notation) Ereignisformat für die Darstellung generischer Ereignisdaten.

Mit dem SEF-Format werden Ereignisse vom ESM-Gerät an einen Empfänger auf einem anderen ESM-Gerät sowie vom ESM-Gerät an Dritte weitergeleitet. Sie können das Format außerdem verwenden, um Ereignisse von Dritten an einen Empfänger zu senden, indem Sie beim Erstellen der Datenquelle SEF als Datenformat auswählen.

Beim Einrichten der Ereignisweiterleitung mit SEF von ESM zu ESM müssen Sie vier Schritte ausführen:

1 Exportieren Sie Datenquellen, benutzerdefinierte Typen und benutzerdefinierte Regeln von dem ESM-Gerät, von dem die Ereignisse weitergeleitet werden.

– Zum Exportieren der Datenquellen folgen Sie den Anweisungen unter *Verschieben von Datenquellen auf ein anderes System*.

– Zum Exportieren der benutzerdefinierten Typen öffnen Sie **Systemeigenschaften**, klicken Sie auf **Benutzerdefinierte Typen** und dann auf **Exportieren**.

– Zum Exportieren der benutzerdefinierten Regeln folgen Sie den Anweisungen unter *Exportieren von Regeln*.

2 Importieren Sie auf dem ESM-Gerät mit dem Empfänger, an den Sie weiterleiten, die gerade exportierten Datenquellen, benutzerdefinierten Typen und benutzerdefinierten Regeln.

– Zum Importieren der Datenquellen folgen Sie den Anweisungen unter *Verschieben von Datenquellen auf ein anderes System*.

– Zum Importieren der benutzerdefinierten Typen öffnen Sie **Systemeigenschaften**, klicken Sie auf **Benutzerdefinierte Typen** und dann auf **Importieren**.

– Zum Importieren der benutzerdefinierten Regeln folgen Sie den Anweisungen unter *Importieren von Regeln*.

3 Fügen Sie auf dem ESM-Gerät, das die Ereignisse von einem anderen ESM-Gerät empfängt, eine ESM-Datenquelle hinzu.

– Klicken Sie in der Systemnavigationsstruktur auf das Empfängergerät, zu dem Sie die Datenquelle hinzufügen möchten, und klicken Sie dann auf das Symbol **Datenquelle hinzufügen**  .

– Wählen Sie auf der Seite **Datenquelle hinzufügen** im Feld **Datenquellenanbieter** die Option **McAfee** und dann im Feld **Datenquellenmodell** die Option **Enterprise Security Manager (SEF)** aus.

– Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

4 Fügen Sie das Ereignisweiterleitungsziel auf dem sendenden ESM-Gerät hinzu.

– Klicken Sie in der Systemnavigationsstruktur auf das System, und klicken Sie dann auf das Symbol **Eigenschaften**  .

– Klicken Sie auf **Ereignisweiterleitung** und dann auf **Hinzufügen**.

– Wählen Sie auf der Seite **Ereignisweiterleitungsziel hinzufügen** im Feld **Format** die Option **Syslog (Standardereignisformat)** aus. Füllen Sie die verbleibenden Felder mit den Informationen für das ESM-Gerät aus, an das Sie weiterleiten, und klicken Sie auf **OK**.

Verwalten von Berichten

In Berichten werden Daten aus den Ereignissen und Flüssen angezeigt, die auf dem ESM-Gerät verwaltet werden. Sie können eigene Berichte entwerfen oder einen der vordefinierten Berichte ausführen und im PDF-, HTML- oder CSV-Format senden.

Vordefinierte Berichte

Die vordefinierten Berichte sind in die folgenden Kategorien unterteilt:

- Compliance
- Management
- McAfee ADM
- McAfee Database Activity Monitoring (DAM)
- McAfee DEM
- McAfee Event Reporter

Mit diesen Berichten werden auf Ereignissen basierende Daten generiert.

Benutzerdefinierte Berichte

Beim Erstellen eines Berichts entwerfen Sie das Layout im **Berichtslayout**-Editor, indem Sie Ausrichtung, Größe, Schriftart, Ränder sowie Kopf- und Fußzeile auswählen. Sie können außerdem Komponenten einschließen und diese so einrichten, dass die Daten nach Ihren Vorstellungen angezeigt werden.

Alle Layouts werden gespeichert und können für mehrere Berichte verwendet werden. Beim Hinzufügen eines Berichts haben Sie die Möglichkeit ein neues Layout zu entwerfen, ein vorhandenes Layout unverändert zu verwenden oder es als Vorlage zu verwenden und seine Funktionen zu bearbeiten. Außerdem können Sie nicht mehr benötigte Berichtslayouts entfernen.

Siehe auch

Hinzufügen einer Berichtsbedingung auf Seite 265
Festlegen des Startmonats für Quartalsberichte auf Seite 264
Hinzufügen eines Berichtslayouts auf Seite 265

Festlegen des Startmonats für Quartalsberichte

Wenn Sie quartalsweise Berichte ausführen, müssen Sie den ersten Monat des ersten Quartals definieren. Wenn der erste Monat definiert und in der Systemtabelle gespeichert ist, werden Berichte quartalsweise auf diesem Startdatum basierend ausgeführt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der ESM-Konsole die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Benutzerdefinierte Einstellungen**.
2. Wählen Sie im Feld **Legen Sie fest, welcher Monat verwendet werden soll** den Monat aus.
3. Klicken Sie auf **Anwenden**, um die Einstellung zu speichern.

Hinzufügen eines Berichts

Fügen Sie Berichte zu ESM hinzu, und legen Sie fest, dass diese regelmäßig in von Ihnen definierten Intervallen oder bei manueller Auswahl ausgeführt werden. Sie können ein vorhandenes Berichtslayout auswählen oder mit dem **Berichtslayout**-Editor ein neues Berichtslayout erstellen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Berichte**.
2. Klicken Sie auf **Hinzufügen**, und definieren Sie dann auf der Seite **Bericht hinzufügen** die Einstellungen.
3. Klicken Sie auf **Speichern**.

Der Bericht wird zur Tabelle auf der Seite **Berichte** hinzugefügt und gemäß den Angaben im Feld **Bedingung** ausgeführt.

Hinzufügen eines Berichtslayouts

Entwerfen Sie das Layout für einen Bericht, wenn die vordefinierten Layouts nicht Ihren Anforderungen entsprechen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Berichte**.
2. Klicken Sie auf **Hinzufügen**, um die Seite **Bericht hinzufügen** zu öffnen, und füllen Sie dann die Abschnitte 1, 2 und 3 aus.
3. Wählen Sie in Abschnitt 4 die Option **Bericht im PDF-Format** oder **Bericht im HTML-Format** aus.
4. Klicken Sie in Abschnitt 5 auf **Hinzufügen**, um den **Berichtslayout**-Editor zu öffnen.
5. Richten Sie das Layout zum Anzeigen der vom Bericht generierten Daten ein.

Das Layout wird gespeichert und kann in dieser Form für andere Berichte oder als Vorlage, die Sie bearbeiten können, verwendet werden.

Einschließen eines Bilds in PDF-Dateien und Berichte

Sie können das ESM-Gerät so einrichten, dass exportierte PDF-Dateien und gedruckte Berichte das auf dem Bildschirm **Anmeldung** angezeigte Bild enthalten.

Bevor Sie beginnen

Fügen Sie das Bild zur Seite **Benutzerdefinierte Einstellungen** hinzu (siehe *Anpassen der Anmeldeseite*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Benutzerdefinierte Einstellungen**.
2. Wählen Sie **Bild in aus Ansichten oder gedruckten Berichten exportierte PDF-Dateien einschließen** aus.
3. Klicken Sie auf **OK**.

Siehe auch

Anpassen der Anmeldeseite auf Seite 22

Hinzufügen einer Berichtsbedingung

Fügen Sie Bedingungen hinzu, damit diese beim Einrichten eines Berichts verfügbar sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Berichte**.
2. Klicken Sie auf **Bedingungen**, und geben Sie dann die erforderlichen Informationen ein.
3. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Diese Option wird in der Liste der verfügbaren Bedingungen angezeigt, wenn Sie die Bedingung für einen Bericht auswählen.

Anzeigen von Host-Namen in einem Bericht

Sie können konfigurieren, dass in Berichten DNS-Auflösung für Quell- und Ziel IP-Adressen verwendet wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften** .
2. Klicken Sie auf **Berichte** und dann auf **Hinzufügen**. Geben Sie in den Abschnitten 1 bis 4 die erforderlichen Informationen ein.
3. Klicken Sie in Abschnitt 5 auf **Hinzufügen**, ziehen Sie eine Komponente (**Tabelle**, **Balkendiagramm** oder **Kreisdiagramm**), legen Sie sie an der gewünschten Stelle ab, und schließen Sie den **Abfragen-Assistenten** ab.
4. Wählen Sie im Abschnitt **Abfrage** des Bereichs **Eigenschaften** im **Berichtslayout**-Editor die Option **IPs in Host-Namen auflösen** aus.

Die Ergebnisse der DNS-Suche werden nicht nur im Bericht angezeigt, sondern Sie können sie auch in der Tabelle **Hosts** anzeigen (**Systemeigenschaften** | **Hosts**).

Beschreibung der *contains*-Filter und Filter für *reguläre Ausdrücke*

Bei den *contains*-Filtern und Filtern für *reguläre Ausdrücke* können Sie sowohl in Daten für Indexzeichenfolgen als auch in Daten für nicht indizierte Zeichenfolgen Platzhalter verwenden. Für die Syntax dieser Filter gelten bestimmte Anforderungen.

Diese Befehle können Sie in jedem Feld verwenden, in dem Text- oder Zeichenfolgendaten zulässig sind. Die meisten Textfelder sind mit dem Symbol für das Ignorieren der Groß-/Kleinschreibung Aa neben dem Namen des Filterfelds gekennzeichnet. Andere Felder, für die `contains` zulässig ist, sind nicht mit diesem Symbol versehen. Die vollständige Liste der Felder finden Sie im Abschnitt *Felder mit Unterstützung der `contains`-Funktion*.

Syntax und Beispiele

Die Basissyntax für contains lautet `contains(beliebigerWert)`, und die für reguläre Ausdrücke lautet `regex(regulärer Ausdruck)`.

Um die Groß-/Kleinschreibung zu ignorieren klicken Sie auf das entsprechende Symbol Aa, oder verwenden Sie die Schreibweise `/i` für reguläre Ausdrücke, beispielsweise `regex(/beliebigerWert/i)`. Durch die Suche werden unabhängig von der Groß-/Kleinschreibung alle Werte zurückgegeben, die `beliebigerWert` enthalten.

Die Symbole NICHT ! und ODER or gelten für die Werte für reguläre Ausdrücke und contains-Werte. Wenn in den Ergebnissen die Werte angezeigt werden sollen, die einen bestimmten Wert nicht enthalten, geben Sie den Wert ein, und klicken Sie auf das Symbol NICHT. Wenn in den Ergebnissen Werte angezeigt werden sollen, die einen oder einen anderen Wert enthalten, geben Sie die Werte ein, und klicken Sie auf das Symbol ODER.

Beispiel 1: Einfache Suche

Indizierte Felder: `contains(stra)`, `regex(stra)`

Nicht indizierte Felder: `stra`

Ergebnis: Gibt alle Zeichenfolgen zurück, die `stra` enthalten, beispielsweise administrator, gmestrad oder straub.

Beispiel 2: Suche mit ODER

Indizierte Felder: `contains(admin,NGCP)`, `regex((admin|NGCP))`

Nicht indizierte Felder: `admin,NGCP`

Ergebnisse: Gibt alle Zeichenfolgen in dem Feld zurück, die admin oder NGCP enthalten. Die zusätzlichen Klammern sind erforderlich, damit der reguläre Ausdruck ODER funktioniert.

Beispiel 3: Suche nach Sonderzeichen wie beispielsweise in Dienstkonten

Dollarzeichen:

Indizierte Felder: `contains($)`, `regex(\x24)` oder `regex(\$)`

Nicht indizierte Felder: `$`

Ergebnisse: In allen Fällen wird jede Zeichenfolge in dem Feld zurückgegeben, die `$` enthält. Unter http://www.ascii.cl finden Sie eine Liste der HEX-Werte für die Zeichen.

Wenn Sie für einen regulären Ausdruck das Zeichen `$` ohne Skalierung verwenden, wird ein leerer Ergebnissatz zurückgegeben. Eine PCRE-Escape-Sequenz ist als Suchmethode besser geeignet.

Prozentzeichen:

Indizierte Felder: `contains(%)`, `regex(\x25)` oder `regex(\%)`

Nicht indizierte Felder: `%`

Umgekehrter Schrägstrich:

Indizierte Felder: `contains(\)`, `regex(\x5c)` oder `regex(\\)`

Nicht indizierte Felder: `\`

Doppelte umgekehrte Schrägstriche

Indizierte Felder: `contains(\\)`, `regex(\x5c\x5c)` oder `regex(\\\)`

Nicht indizierte Felder: `\\`

In manchen Fällen wird möglicherweise, wenn Sie für den regulären Ausdruck nicht den HEX-Wert oder den Schrägstrich verwenden, der Fehler *Ungültiger regulärer Ausdruck (ER5-0015)* angezeigt.

Beispiel 4: Suche mit dem Platzhalter *

Indizierte Felder: `contains (ad*)`

Nicht indizierte Felder: `ad*`

Ergebnisse: Gibt alle Zeichenfolgen zurück, die mit `ad` beginnen, beispielsweise administrator und address.

Beispiel 5: Suche mit regulärem Ausdruck

```
regex(nitroguard/x28[3-4]/x29[com|info}+)

(3)www(10)nitroguard(3)com(0)

(3)www(10)nitroguard(4)info(0)

(3)www(10)nitroguard(3)gov(0)

(3)www(10)nitroguard(3)edu(0)

(3)www(10)nitroguard(7)oddball(0)
```

Diese Domänen stammen aus Microsoft DNS-Ereignissen.

Ergebnisse: Mit diesem regulären Ausdruck wird eine bestimmte Zeichenfolge ausgewählt. In diesem Fall ist dies `nitroguard`, eine drei- oder vierstellige primäre Domäne und `com` oder `info`. Mit diesem regulären Ausdruck stimmen die ersten beiden Ausdrücke überein, die anderen jedoch nicht. Diese Beispiele sollen veranschaulichen, wie Sie reguläre Ausdrücke mit der Funktion verwenden können. Ihre Ausdrücke werden völlig anders aussehen.

Beachten Sie dabei jedoch Folgendes:

- Wenn Sie `reguläre Ausdrücke` mit Werten aus weniger als drei Zeichen verwenden, führt dies zu einem höheren Overhead und einer langsameren Abfrageleistung. Es wird vorgeschlagen, nur Abfragen mit mehr als drei Zeichen zu verwenden.
- Dieser Filter kann nicht in Korrelationsregeln oder Alarmen verwendet werden. Als einzige Ausnahme kann der Filter in Korrelationsregeln mit benutzerdefinierten Typen für Name/Wert verwendet werden.
- Wenn Sie `contains` oder einen `regulären Ausdruck` zusammen mit NICHT verwenden, kann dies zu einem höheren Overhead und einer langsameren Abfrageleistung führen.

Beschreibung für Bloom-Filter

Informationen zu Bloom-Filtern finden Sie unter http://en.wikipedia.org/wiki/Bloom_filter

Felder mit Unterstützung der `contains`-Funktion und der Funktion für `reguläre Ausdrücke`

Access_Resource	File_Operation_Succeeded	Referenz
Anwendung	File_Path	Registry_Key
Application_Protocol	File_Type	Registry_Value
Bereich	Dateiname	Request_Type
Authoritative_Answer	Forwarding_Status	Response_Code
Bcc	Von	Return_Code
Caller_Process	From_Address	RTMP_Application
Catalog_Name	FTP_Command	Sensor_Name
Kategorie	Host	Sensor_Type
Cc	HTTP_Req_Cookie	Sensor_UUID
Client_Version	HTTP_Req_Host	Session_Status
Befehl	HTTP_Req_Method	Signatur-ID

Contact_Name	HTTP_Req_Referer	Signature_Name
Contact_Nickname	HTTP_Req_URL	SNMP_Error_Code
Cookie	HTTP_User_Agent	SNMP_Item
Creator_Name	Incomtin_ID	SNMP_Item_Type
Database_ID	Schnittstelle	SNMP_Operation
Database_Name	Interface_Dest	SNMP_Version
Datacenter_ID	Job_Name	Quellbenutzer
Datacenter_Name	Job_Type	Source_Context
DB2_Plan_Name	Sprache	Source_Logon_ID
Delivery_ID	Local_User_Name	Source_Network
Beschreibung	Logical_Unit_Name	Source_UserID
Zielbenutzer	Logon_Type	Source_Zone
Destination_Directory	LPAR_DB2_Subsystem	SQL_Command
Destination_Filename	Mail_ID	SQL_Statement
Destination_Hostname	Postfach	Step_Count
Destination_Logo_ID	Mainframe_Job_Name	Step_Name
Destination_Network	Malware_Insp_Action	Betreff
Destination_UserID	Malware_Insp_Result	SWF_URL
Destination_Zone	Management_Server	Table_Name
Detection_Method	Message_ID	Target_Class
Device_Action	Message_Text	Target_Context
Richtung	Methode	Target_Process_Name
Verzeichnis	NTP_Client_Mode	TC_URL
DNS_Class	NTP_Opcode	Threat_Category
DNS_Name	NTP_Request	Threat_Handled
DNS_Type	NTP_Server_Mode	Threat_Name
Domäne	Objekt	An
Event_Class	Object_Type	To_Address
External_Application	Operating_System	URL
External_DB2_Server	Policy_Name	URL_Category
External_Hostname	Privileged_User	User_Agent
External_SessionID	Process_Name	User_Nickname
Einrichtung	Query_Response	Version
File_Operation	Grund	Virtual_Machine_ID
		Virtual_Machine_Name

Für diese benutzerdefinierten Typen können Sie `contains` und `reguläre Ausdrücke` verwenden:

Ansichten
- Zeichenfolge
- Zufällige Zeichenfolge
- Name/Wert
- Zeichenfolgen-Hashes

Fallverwaltung
- Hinweise
- Zusammenfassung
- Verlauf

Arbeiten mit ESM-Ansichten

Mit ESM werden von einem Gerät protokollierte Informationen zu Ereignissen, Flüssen, Ressourcen und Schwachstellen abgerufen. Die Informationen werden korreliert und in das MSEAC-Modul (McAfee Security Event Aggregation and Correlation) eingefügt.

Inhalt

- *Verwenden von ESM-Ansichten*
- *Anzeigen von Sitzungsdetails*
- *Ansichtssymbolleiste*
- *Vordefinierte Ansichten*
- *Hinzufügen einer benutzerdefinierten Ansicht*
- *Ansichtskomponenten*
- *Arbeiten mit dem Abfragen-Assistenten*
- *Ansichten verwalten*
- *Untersuchen der umliegenden Ereignisse eines Ereignisses*
- *Anzeigen der Details zur IP-Adresse eines Ereignisses*
- *Ändern der Standardansicht*
- *Filtern von Ansichten*
- *Überwachungslisten*
- *Zeichenfolgennormalisierung*

Verwenden von ESM-Ansichten

Die vom ESM-Gerät abgerufenen Daten können mit dem MSEAC-Modul in einer leistungsstarken und flexiblen Berichtanzeige analysiert und überprüft werden. Diese Anzeige befindet sich im mittleren Abschnitt der ESM-Konsole. Dort werden die Daten für die Geräte angezeigt, die Sie in der Systemnavigationsstruktur ausgewählt haben.

Beim Starten der ESM-Konsole wird die Standardansicht angezeigt (siehe *Ändern der Standardansicht*). Sie können die Ansichtsfunktionen verwenden, um eine andere vordefinierte Ansicht auszuwählen (siehe *Vordefinierte Ansichten*) oder eine neue Ansicht zu erstellen (siehe *Hinzufügen einer benutzerdefinierten Ansicht*) und eine Abfrage auszuführen, mit der Sie Ereignisse im Netzwerk anzeigen können (siehe *Ansichtssymbolleiste*). Außerdem können Sie die verschiedenen Optionen der Ansichtssymbolleiste, des Komponentenmenüs und der Komponenten-Symbolleiste für Interaktionen mit den Ansichten und den darin enthaltenen Daten verwenden.

Bei Ausführung einer Abfrage wird in jeder Komponente des Ansichtsbereichs eine Statusanzeige angezeigt. Wenn Sie den Cursor über die Statusanzeige bewegen, wird angezeigt, wie viel Zeit bei der Ausführung der Abfragen der einzelnen Komponenten verstrichen ist und wie viel Prozent dies entspricht. Wenn Sie eine Abfrage abbrechen möchten, um ESM-Ressourcen freizugeben, klicken Sie auf das Löschsymbol rechts neben der Statusanzeige.

Die nicht festgelegten Werte oder aggregierten Werte für Quell-IP-Adresse und Ziel-IP-Adresse werden in allen Ergebnissätzen einer Ansicht als "::" anstelle von "0.0.0.0" angezeigt. Beispiel: ::ffff:10.0.12.7 wird als 0:0:0:0:0:FFFF: A00:C07 eingefügt (A00:C07 entspricht 10.0.12.7), ::0000:10.0.12.7 entspricht 10.0.12.7.

Anzeigen von Sitzungsdetails

In der **Sitzungsanzeige** können Sie die Details eines Ereignisses mit einer Sitzungs-ID anzeigen und in einer CSV-Datei speichern.

Nur Ereignisse, die sich in einer Sitzung befinden, haben eine Sitzungs-ID. Eine Sitzung ist das Ergebnis einer Verbindung zwischen einer Quelle und einem Ziel. Ereignisse, die intern im Gerät oder in ESM stattfinden, haben keine Sitzungs-IDs.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Dropdown-Liste mit den Ansichten die Ansicht aus, die die anzuzeigende Sitzung enthält.
2. Wählen Sie das Ereignis aus, klicken Sie auf der Titelleiste der Komponente auf das Menüsymbol, und wählen Sie dann Folgendes aus: **Ereignis-Drilldown** | **Ereignisse**.
3. Klicken Sie auf das Ereignis, auf die Registerkarte **Erweiterte Details** und dann auf das Symbol **Sitzungsdaten anzeigen** neben dem Feld **Sitzungs-ID**.

Die **Sitzungsanzeige** wird geöffnet, und die Details der Sitzung werden angezeigt.

Ansichtssymbolleiste

Die Ansichtssymbolleiste befindet sich oben im Ansichtsbereich und enthält verschiedene Optionen, die Sie beim Einrichten der Ansichten verwenden.

Tabelle 7-1



Option	Beschreibung
1 — **Gerätestruktur ausblenden**	Klicken Sie auf diese Option, um die aktuelle Ansicht zu erweitern, indem Sie den Bereich der Gerätestruktur ausblenden.
2: Navigation anzeigen	Navigieren Sie zwischen vorherigen Ansichten vor und zurück.
3: Liste anzeigen	Wählen Sie eine Ansicht in der Dropdown-Liste aus, in der alle vordefinierten und benutzerdefinierten Ansichten aufgeführt werden, die für die Anzeige in dieser Liste ausgewählt sind.
4 — **Ansichten verwalten**	Verwalten Sie alle Ansichten (siehe *Verwalten der Ansichten*). Sie können auswählen, welche Ansichten in der Liste der Ansichten enthalten sein sollen, Ordner hinzufügen und Ansichten umbenennen, löschen, kopieren, importieren und exportieren.
5 — **Aktuelle Ansicht aktualisieren**	Aktualisieren Sie alle Daten, die zurzeit im Ansichtsbereich angezeigt werden.

Tabelle 7-1



(Fortsetzung)

Option	Beschreibung
6: Standardansicht	Wechseln Sie zurück zur Standardansicht.
7 — **Aktuelle Ansicht drucken**	Drucken Sie eine Kopie der aktuellen Ansicht. Folgende Druckoptionen stehen zur Verfügung: • **Alle Komponenten an eine Seite anpassen**: Die in der Ansicht enthaltenen Komponenten werden so angepasst, dass die Ansicht auf eine Seite passt. • **Jede Komponente auf einer separaten Seite drucken**: Jede in der Ansicht enthaltene Komponente wird auf einer separaten Seite gedruckt. Wenn Sie auf **Passt die Komponente an die Seite an** klicken, wird die Größe jeder Komponente so angepasst, dass die Seite ausgefüllt ist. • **Nur sichtbaren Bereich drucken**: Nur der auf dem Bildschirm sichtbare Teil der Ansicht wird gedruckt. • **In PDF-Datei exportieren**: Die Ansicht wird als PDF-Datei gespeichert.
8 — **Aktuelle Ansicht bearbeiten**	Ändern Sie die zurzeit angezeigte Ansicht, wenn es sich um eine benutzerdefinierte Ansicht handelt. Wenn Sie auf diese Option klicken, wird die **Symbolleiste zum Bearbeiten von Ansichten** geöffnet (siehe *Erstellen einer benutzerdefinierten Ansicht*).
9 — **Neue Ansicht erstellen**	Erstellen Sie eine neue benutzerdefinierte Ansicht (siehe *Erstellen einer benutzerdefinierten Ansicht*).
10: Zeitraum	Legen Sie den Zeitraum für die Informationen fest, die in der Ansicht angezeigt werden sollen.
11 — **Filter ausblenden**	Klicken Sie auf diese Option, um die aktuelle Ansicht zu erweitern, indem Sie den Filterbereich ausblenden.

Vordefinierte Ansichten

Über die Dropdown-Liste auf der Ansichtssymbolleiste können Sie auf die im Umfang des Systems enthaltenen Ansichten sowie auf selbst hinzugefügte benutzerdefinierte Ansichten zugreifen.

Die folgenden vordefinierten Ansichten stehen zur Verfügung.

- In den Ansichten **Ressource, Bedrohung und Risiko** werden Daten zu Ressourcen, Bedrohungen und Risiken sowie deren mögliche Auswirkungen auf das System zusammengefasst und angezeigt.
- **Compliance-Ansichten**: Werden bei der Optimierung von Aktivitäten im Zusammenhang mit der Vorschriften-Compliance verwendet.
- **Dashboard-Ansichten**: Hier erhalten Sie eine Übersicht über bestimmte Aspekte des Systems.

- **Gerätestatus**: Hier wird der Status der in der Systemnavigationsstruktur ausgewählten Geräte angezeigt. Wenn Sie in der Ansicht auf ein Gerät klicken, werden in der unteren Hälfte der Ansicht die Integritätsinformationen für das ausgewählte Gerät angezeigt.
- **Erweiterte ELM-Suche**: Hier können Sie den Fortschritt und die Ergebnisse der Suche in Echtzeit verfolgen. Diese Ansicht ist nur verfügbar, wenn im System ein ELM-Gerät vorhanden ist (siehe *Ansicht Erweiterte ELM-Suche*).
- **Ereignisansichten**: Hier werden die Informationen unterteilt dargestellt, die von Ereignissen im Zusammenhang mit dem in der Systemnavigationsstruktur ausgewählten Gerät generiert wurden.
- **Management-Ansichten**: Hier erhalten Sie eine Übersicht über Aspekte des Systems, die vor allem für Mitarbeiter außerhalb des IT-Bereichs von Interesse sind.
- **Flussansichten**: Hier werden die Informationen unterteilt dargestellt, die zu den einzelnen Flüssen (oder Verbindungen) über Nitro IPS aufgezeichnet wurden (siehe *Flussansichten*).
- **McAfee Event Reporter**: Enthält produktspezifische Ansichten für zahlreiche McAfee-Produkte.
- **Risiko-Ansichten**: Werden mit dem ACE-Standard-Manager verwendet. Um Daten für benutzerdefinierte Manager richtig anzuzeigen, müssen Sie benutzerdefinierte Ansichten erstellen.
- **Workflow-Ansichten für Ereignisse** enthält die folgenden Ansichten:
  - **Ausgelöste Alarme**: Hier können Sie die Alarme anzeigen und verwalten, die ausgelöst wurden, da Alarmbedingungen erfüllt waren (siehe Ansicht *Ausgelöste Alarme*).
  - **Fallverwaltung**: Hier können Sie die Fälle im System anzeigen und verwalten (siehe *Anzeigen aller Fälle*).

Flussansichten

Ein *Fluss* ist ein Datensatz für eine über das Gerät hergestellte Verbindung. Wenn die Flussanalyse auf dem Nitro IPS-Gerät aktiviert ist, werden Daten zu allen über das Nitro IPS-Gerät erfolgten Flüsse oder Verbindungen aufgezeichnet.

Flüsse haben Quell- und Ziel-IP-Adressen, Quell- und Zielports, Quell- und Ziel-MAC-Adressen, ein Protokoll sowie eine Angabe für Erstes Mal und Letztes Mal (als Hinweis auf den Zeitraum zwischen Anfang und Ende der Verbindung).

Da Flüsse keinen Hinweis auf anomalen oder bösartigen Datenverkehr darstellen, sind mehr Flüsse als Ereignisse vorhanden. Im Gegensatz zu einem Ereignis ist ein Fluss nicht einer Regelsignatur (SigID) zugeordnet. Flüsse sind nicht Ereignisaktionen wie Warnung, Verwerfen und Ablehnen zugeordnet.

Bestimmte Daten beziehen sich eindeutig auf Flüsse. Dazu gehören Quell- und Ziel-Bytes sowie Quell- und Zielpakete. Bei *Quell-Bytes* und *Quellpaketen* handelt es sich um die Anzahl der Bytes und Pakete, die von der Quelle des Flusses übermittelt wurden. Die *Ziel-Bytes* und *Zielpakete* stellen die Anzahl der Bytes und Pakete dar, die vom Ziel des Flusses übermittelt wurden. Flüsse haben eine Richtung: Ein *eingehender Fluss* ist definiert als ein Fluss, dessen Ursprung sich außerhalb des Heimnetzwerks (HOME_NET) befindet. Ein *ausgehender Fluss* hat seinen Ursprung innerhalb des Heimnetzwerks (HOME_NET). Diese Variable wird in einer Richtlinie für ein Nitro IPS-Gerät definiert.

Zum Anzeigen von Flussdaten müssen Sie die Protokollierung von Flussdaten im System aktivieren. Dann können Sie Flüsse in der Ansicht **Flussanalyse** anzeigen.

Aktivieren der Flussprotokollierung

Zum Anzeigen von Flussanalysedaten für ein Nitro IPS-Gerät müssen Sie zwei Firewall-Variablen aktivieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur ein Gerät aus.

2 Klicken Sie auf das Symbol **Richtlinien-Editor**  , und wählen Sie dann im Bereich **Regeltypen** die Option **Variable** aus.

3 Erweitern Sie im Regelanzeigebereich die Kategorie **Firewall**.

4 Heben Sie in der Zeile **INBOUND_CONNECTION_STATISTICS** die Auswahl von **Vererben** auf, um die Vererbung des Werts zu unterbrechen. Geben Sie dann `Ja` ein, und klicken Sie auf **OK**.

5 Heben Sie für **OUTBOUND_CONNECTION_STATISTICS** die Auswahl von **Vererben** auf, um die Vererbung des Werts zu unterbrechen. Geben Sie dann `Ja` ein, und klicken Sie auf **OK**.

Ansicht Erweiterte ELM-Suche

Die Ansicht **Erweiterte ELM-Suche** ist verfügbar, wenn im System mindestens ein ELM-Gerät vorhanden ist. Mit dieser Ansicht können Sie detailliertere Suchvorgänge ausführen und beim Durchsuchen von Protokollen auf einem oder mehreren ELM-Geräten den Suchfortschritt und die Ergebnisse in Echtzeit verfolgen.

In dieser Ansicht werden die Funktionen des Archivs auf dem ELM-Gerät für die Erstellung von Statistikberichten genutzt. Sie erhalten Echtzeitinformationen zur Menge der zu durchsuchenden Daten und können die Abfrage eingrenzen, um die Anzahl der durchsuchten Dateien zu minimieren.

Um die Geschwindigkeit der Suche bei Verwendung von **Erweiterte ELM-Suche** zu erhöhen, müssen Sie das Scan-Modul für die Volltextindizierung aktivieren. Dadurch wird die Geschwindigkeit erhöht, da weniger Dateien durchsucht werden müssen. Damit diese Steigerung wirksam wird, müssen alle vorhandenen ELM-Protokolle indiziert werden. Nach der Aktivierung der Indizierung kann dieser Vorgang mehrere Wochen dauern. Ausschlaggebend sind dabei die Geschwindigkeit des Systems und die Anzahl der erfassten Protokolle. Die Suchleistung wird in dieser Zeit nicht verringert, vielmehr wird sie durch die Indizierung der ELM-Protokolle verbessert. Informationen zum Aktivieren der Volltextindizierung finden Sie unter *Ermöglichen schnellerer ELM-Suchvorgänge*.

Während des Suchvorgangs werden in den Diagrammen die geschätzten Ergebnisse angezeigt:

- Diagramm **Zeitliche Verteilung der Ergebnisse**: Hier werden die Schätzungen und Ergebnisse basierend auf einer zeitlichen Verteilung angezeigt. Die untere Achse ändert sich abhängig von der Auswahl in der Dropdown-Liste für den Zeitraum.
- Diagramm **Ergebnisse für Datenquelle**: Hier werden die Schätzungen und Ergebnisse pro Datenquelle basierend auf den Datenquellen der in der Systemnavigationsstruktur ausgewählten Geräte angezeigt.
- Diagramm **Ergebnisse für Gerätetyp**: Hier werden die Schätzungen und Ergebnisse pro Gerätetyp basierend auf den in der Systemnavigationsstruktur ausgewählten Geräten angezeigt.

Die Diagramme werden vor Beginn der Suche ausgefüllt und aktualisiert, wenn Ergebnisse gefunden werden. Sie können auf der Seite **Ergebnisse für Datenquelle** oder **Ergebnisse für Gerätetyp** einen oder mehrere Balken auswählen oder einen Abschnitt des Diagramms **Zeitliche Verteilung der Ergebnisse** hervorheben. Klicken Sie auf **Filter anwenden**, um die Suche einzuengen, sobald die ersten Ergebnisse eingehen. Auf diese Weise können Sie die Suchergebnisse weiter aufgliedern und die Menge der zu durchsuchenden Daten begrenzen. Nach Abschluss der Suche werden in den Diagrammen die tatsächlichen Ergebnisse angezeigt.

Ausführen einer erweiterten ELM-Suche

Durchsuchen Sie die Protokolle eines oder mehrerer ELM-Geräte nach Informationen, die Sie definieren. Wenn die Volltextindizierung aktiviert ist, wird die ELM-Suche beschleunigt, da weniger Dateien durchsucht werden müssen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im Ansichtsbereich in der Dropdown-Liste die Option **Erweiterte ELM-Suche** aus.

2 Wenn mehrere ELM-Geräte im System vorhanden sind, wählen Sie die Geräte für die Suche in der Dropdown-Liste neben dem Textfeld aus.

3 Geben Sie eine normale Textsuche oder einen regulären Ausdruck in das Textfeld ein.



Das Vokabular für die Volltextindizierung (beispielsweise *XOR* und *NOT*) wird in diesem Feld nicht unterstützt. Die Operatoren *AND* und *OR* werden unterstützt.

4 Wenn Sie einen anderen Zeitraum als **Aktueller Tag** verwenden möchten, wählen Sie diesen in der Dropdown-Liste aus.

5 Wählen Sie in der Systemnavigationsstruktur die zu durchsuchenden Geräte aus.

6 Wählen Sie bei Bedarf eine oder mehrere der folgenden Optionen aus:

- **Groß-/Kleinschreibung ignorieren**: Die Groß-/Kleinschreibung wird bei der Suche ignoriert.
- **Regulärer Ausdruck**: Der Begriff im Suchfeld wird als regulärer Ausdruck behandelt.
- **Enthält NICHT den Suchbegriff**: Gibt Übereinstimmungen zurück, die den Begriff im Suchfeld nicht enthalten.

7 Klicken Sie auf **Suchen**.

Die Ergebnisse werden im Abschnitt **Suchergebnisse** der Ansicht angezeigt.

8 Führen Sie während der Suche oder nach Abschluss der Suche einen oder mehrere der folgenden Schritte aus.

Option	Beschreibung
Suche speichern 	Mit dieser Option werden die Ergebnisse der Suche gespeichert, auch wenn Sie die Ansicht verlassen. Gespeicherte Suchvorgänge können Sie auf der Seite **ELM-Eigenschaften** | **Daten** den Umgehungsmodus für das Gerät zu deaktivieren.
Datei mit Suchergebnissen herunterladen 	Laden Sie die Ergebnisse an den von Ihnen festgelegten Speicherort herunter.
Ausgewählte Elemente in die Zwischenablage kopieren 	Kopieren Sie die ausgewählten Elemente in die Zwischenablage, damit Sie sie in ein anderes Dokument einfügen können.
Datendetails anzeigen 	Zeigen Sie Details für Protokolle an, die Sie in der Tabelle **Suchergebnisse** auswählen.

Anzeigen und Verwalten von ausgelösten Alarmen

In dieser Ansicht werden ausgelöste und nicht gelöschte Alarme aufgeführt. Sie können verschiedene Aktionen ausführen, um die Alarme zu verwalten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der ESM-Konsole das Schnellstartsymbol für **Alarme** aus, um die Ansicht **Ausgelöste Alarme** zu öffnen.

2 Führen Sie eine der folgenden Aktionen aus:

Aufgabe	Vorgehensweise
Bestätigen eines Alarms	• Zum Bestätigen eines Alarms klicken Sie auf das Kontrollkästchen in der ersten Spalte des ausgelösten Alarms, den Sie bestätigen möchten. • Zum Bestätigen mehrerer Alarme heben Sie die Elemente hervor, und klicken Sie dann unten in der Ansicht auf das Symbol **Alarm bestätigen**. Bestätigte Alarme werden aus dem Bereich **Alarme** entfernt, sind jedoch in der Ansicht **Ausgelöste Alarme** weiterhin enthalten.
Löschen eines Alarms aus dem System	• Wählen Sie den zu löschenden ausgelösten Alarm aus, und klicken Sie dann auf das Symbol **Alarm löschen**.
Filtern der Alarme	• Geben Sie im Bereich **Filter** die Informationen ein, die Sie als Filter verwenden möchten, und klicken Sie dann auf das Symbol **Aktualisieren**.
Ändern des Beauftragten für Alarme	1 Wenn die Registerkarten mit den Datendetails nicht unten in der Ansicht angezeigt werden, klicken Sie auf das Symbol **Datendetails anzeigen**. 2 Wählen Sie die Alarme aus, klicken Sie dann auf **Beauftragter**, und wählen Sie den neuen Beauftragten aus.
Erstellen eines Falls für Alarme	1 Stellen Sie sicher, dass die Registerkarten mit den Datendetails angezeigt werden. 2 Wählen Sie die Alarme aus, klicken Sie dann auf **Fall erstellen**, und wählen Sie die benötigten Optionen aus.

Aufgabe	Vorgehensweise
Anzeigen von Details zu einem Alarm	1 Stellen Sie sicher, dass die Registerkarten mit den Datendetails unten in der Ansicht angezeigt werden. 2 Wählen Sie den Alarm aus, und führen Sie eine der folgenden Aktionen aus: • Klicken Sie auf die Registerkarte **Auslösendes Ereignis**, um das Ereignis anzuzeigen, durch das der ausgewählte Alarm ausgelöst wurde. Doppelklicken Sie auf das Ereignis, um eine Beschreibung anzuzeigen. Die Registerkarte **Auslösendes Ereignis** ist nicht immer verfügbar, da einige Alarmbedingungen nicht von einem einzelnen Ereignis erfüllt werden. • Klicken Sie auf die Registerkarte **Bedingung**, um die Bedienung anzuzeigen, durch die das Ereignis ausgelöst wurde. • Klicken Sie auf die Registerkarte **Aktion**, um die als Ergebnis des Alarms ausgeführten Aktionen und die dem Ereignis zugewiesenen ePolicy Orchestrator-Tags anzuzeigen.
Bearbeiten der Einstellungen für ausgelöste Alarme	1 Klicken Sie auf den ausgelösten Alarm, klicken Sie dann auf das Symbol **Menü**, und wählen Sie **Alarm bearbeiten** aus. 2 Nehmen Sie auf der Seite **Alarmeinstellungen** die Änderungen vor (klicken Sie auf den einzelnen Registerkarten auf das Symbol **Hilfe**, um Anweisungen anzuzeigen), klicken Sie dann auf **Fertig stellen**.

Hinzufügen einer benutzerdefinierten Ansicht

Benutzerdefinierte Ansichten enthalten Komponenten, mit denen Sie die gewünschten Informationen anzeigen können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf der Ansichtssymbolleiste auf das Symbol **Neue Ansicht erstellen**. Klicken Sie dann auf der **Symbolleiste zum Bearbeiten von Ansichten** auf eine Komponente, und ziehen Sie sie an die gewünschte Stelle (siehe *Ansichtskomponenten*).

2 Nehmen Sie im **Abfragen-Assistenten** eine Auswahl vor, sodass in der Ansicht die anzuzeigenden Daten generiert werden (siehe *Arbeiten mit dem **Abfragen-Assistenten***). Klicken Sie dann auf **Fertig stellen**.

Die Daten werden in der hinzugefügten Komponente angezeigt.

3 Führen Sie einen oder mehrere der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Verschieben der Komponente	Klicken Sie auf die Titelleiste der Komponente, ziehen Sie sie an die gewünschte Stelle, und legen Sie sie ab.
Standardmäßiges Anzeigen von Host-Namen anstelle von IP-Adressen	Klicken Sie auf der Symbolleiste einer Komponente, in der IP-Adressen angezeigt werden, auf das Symbol **Hostnamen anzeigen** (siehe *Verwalten von Hostnamen*).
Anpassen der Komponente	Klicken Sie auf die Komponente, und nehmen Sie Änderungen an den Einstellungen im Bereich **Eigenschaften** vor (siehe *Anpassen von Komponenten*).

Aufgabe	Vorgehensweise
Hinzufügen weiterer Komponenten zur Ansicht	1 Klicken Sie auf eine Komponente, und ziehen Sie sie an die gewünschte Stelle. 2 Nehmen Sie im **Abfragen-Assistenten** eine Auswahl vor, sodass in der Ansicht die anzuzeigenden Daten generiert werden. Klicken Sie dann auf **Fertig stellen**.
Speichern der Ansicht	1 Klicken Sie auf **Speichern** oder **Speichern unter**, und geben Sie einen Namen für die Ansicht ein. Zum Speichern der Ansicht in einem vorhandenen Ordner wählen Sie den Ordner aus. 2 Klicken Sie auf **OK**.
Kopieren und Einfügen einer Komponente	1 Klicken Sie auf die zu kopierende Komponente. 2 Klicken Sie auf **Kopieren** und dann auf **Einfügen**.
Löschen einer Komponente	Wählen Sie die Komponente aus, und klicken Sie dann auf **Löschen**.
Beenden des Ansichts-Editors ohne Speichern einer Ansicht	Löschen Sie alle Komponenten, und schließen Sie dann die **Symbolleiste zum Bearbeiten von Ansichten**.

Ansichtskomponenten

Erstellen Sie benutzerdefinierte Ansichten, um Daten für Ereignisse, Flüsse, Ressourcen und Schwachstellen auf die für Sie sinnvollste Weise anzuzeigen.

Jede Ansicht besteht aus Komponenten, die Sie auf der **Symbolleiste zum Bearbeiten von Ansichten** auswählen und einrichten, um die Daten anzuzeigen. Wenn Sie eine Komponente auswählen, wird der **Abfragen-Assistent** geöffnet. Hier können Sie Details zu den in der Komponente angezeigten Daten definieren.

Beschreibung der Ansichtskomponenten

Sie können zu einer benutzerdefinierten Ansicht 13 verschiedene Komponenten hinzufügen. Mit diesen können Sie die Ansicht so einrichten, dass die Daten im besten Format angezeigt werden.

Komponente	Beschreibung
 **Messuhr**	Zeigt die Daten auf einen Blick an. Diese Ansicht ist dynamisch und kann mit anderen Komponenten in der Konsole verknüpft werden. Bei Interaktionen mit der ESM-Konsole wird die Ansicht aktualisiert. Jede Skala enthält eine Basislinienanzeige (). Die Farbverläufe entlang des äußeren Rands der Skala wechseln oberhalb der Basislinienanzeige zu Rot. Optional kann sich die Farbe der gesamten Skala ändern, um anomales Verhalten darzustellen: Die Farbe wechselt zu Gelb, wenn das Verhalten innerhalb eines bestimmten Schwellenwerts einer Basislinie liegt, oder zu Rot, wenn der Schwellenwert überschritten wird. Mit der Option **Rate** können Sie die Rate der angezeigten Daten anpassen. Wenn Sie beispielsweise **Aktueller Tag** und **Ereignisse insgesamt** anzeigen und die Rate in Stunde ändern, sehen Sie die Anzahl der Ereignisse pro Stunde für den jeweiligen Tag. Diese Option ist deaktiviert, wenn die angezeigte Abfrage bereits einen Durchschnitt darstellt, beispielsweise **Durchschnitt für Schweregrad** oder **Durchschnitt für Bytes**.
 **Quell- und Zieldiagramm**	Zeigt eine Übersicht über die Aktivitäten für IP-Adressen von Ereignissen oder Flüssen an. Mit der Option Ereignis können Sie IP-Adressen angeben und alle Angriffe auf die angegebenen IP-Adressen anzeigen. Außerdem können Sie alle Angriffe anzeigen, die von den angegebenen IP-Adressen auf andere IP-Adressen ausgeführt wurden. Mit der Option Fluss können Sie IP-Adressen angeben und die IP-Adressen anzeigen, über die Verbindungen mit diesen IP-Adressen hergestellt wurden. Darüber hinaus können Sie die Verbindungen anzeigen, die über die IP-Adressen hergestellt wurden. Dieses Diagramm enthält unten in jeder Komponente ein offenes Feld, in dem Sie die Quell- und Zielereignisse oder -flüsse für eine bestimmte IP-Adresse anzeigen können. Geben Sie die Adresse in das Feld ein, oder wählen Sie eine zuvor verwendete Adresse aus, und klicken Sie dann auf das Symbol **Aktualisieren**  .
 **Kreisdiagramm**	Zeigt die abgefragten Informationen in einem Kreisdiagramm an. Diese Option ist hilfreich, wenn weniger Kategorien zum Anzeigen vorhanden sind (beispielsweise bei einer Protokoll- oder Aktionsabfrage).
 **Tabelle**	Zeigt die Abfrageinformationen in mehreren Spalten an. Diese Komponente ist hilfreich, um Ereignis- und Flussdaten so detailliert wie möglich anzuzeigen.
 **Balkendiagramm**	Zeigt die abgefragten Informationen in einem Balkendiagramm an, in dem Sie die Größe der einzelnen Ergebnisse in einem bestimmten Zeitbereich vergleichen können.
 **Liste**	Zeigt die ausgewählten Abfragedaten im Listenformat an. Diese Komponente ist hilfreich, wenn Sie eine detailliertere Liste mit Elementen in einem kleineren Bereich anzeigen möchten.
 **Verteilung**	Zeigt die Verteilung von Ereignissen und Flüssen in einem Zeitraum an. Sie können Intervalle festlegen, um bestimmte Zeitsegmente zu betrachten und die Daten zu formen.
 **Hinweisbereich**	Diese leere Komponente wird für textbasierte Hinweise verwendet. Sie können Hinweise eingeben, die sich auf die aktuelle Ansicht beziehen.

Komponente	Beschreibung
 **Anzahl**	Zeigt die Gesamtanzahl der Ereignisse, Ressourcen, Schwachstellen oder Flüsse an, die für eine bestimmte Ansicht abgefragt werden.
 **Titel**	Hier können Sie einen Titel oder eine Überschrift für die Ansicht erstellen. Den Titel können Sie an einer beliebigen Stelle in der Ansicht platzieren.
 **Netzwerktopologie**	Hier können Sie die Daten als Darstellung für das gesamte Netzwerk anzeigen. Außerdem können Sie eine benutzerdefinierte Ansicht erstellen, die zusammen mit Netzwerkerkennungsdaten verwendet werden kann (siehe *Hinzufügen von Geräten zur Netzwerktopologie-Komponente*).
 **Geolocation-Übersicht**	Zeigt Ziel- und Quellspeicherort von Warnungen und Flüssen in einer Geolocation-Übersicht an. Über die Optionen in dieser Komponente können Sie mit der **STRG**-Taste und der **UMSCHALTTASTE** wahlweise Ort, Bundesland, Land und Weltregion markieren, die Anzeige vergrößern und verkleinern und Standorte auswählen.
 **Filterliste**	Zeigt eine Liste der Benutzer und Gruppen in Active Directory an. Wenn die Komponente **Filterliste** hinzugefügt wurde, können Sie andere Komponenten an sie binden, indem Sie in **Abfragen-Assistent** in den Filterfeldern **Quellbenutzer** oder **Zielbenutzer** auf den Pfeil nach unten klicken und **Binden an Active Directory-Liste** auswählen. Außerdem können Sie zu **Active Directory** zugeordnete Ereignis- und Flussdaten anzeigen, indem Sie auf das Symbol Menü klicken.

Anpassen von Komponenten

Beim Hinzufügen oder Bearbeiten einer Komponente stehen im Bereich **Eigenschaften** verschiedene Optionen zur Verfügung, mit denen Sie die Komponente anpassen können. Die verfügbaren Optionen hängen von der ausgewählten Komponente ab.

Option	Beschreibung
Titel	Ändern Sie den Titel einer Komponente.
Breite und Höhe	Legen Sie die Abmessungen der Komponente fest. Sie können auch auf die Begrenzungslinie klicken und sie an die gewünschte Stelle ziehen.
X und Y	Legen Sie die Position der Komponente in der Ansicht fest. Sie können auch auf die Titelleiste der Komponente klicken und sie dann an die gewünschte Stelle ziehen und ablegen.
Abfrage bearbeiten	Nehmen Sie Änderungen an der aktuellen Abfrage vor. Wenn Sie auf diese Schaltfläche klicken, wird der **Abfragen-Assistent** geöffnet (siehe *Arbeiten mit dem **Abfragen-Assistenten***).
Steuerungsleiste anzeigen	Legen Sie fest, ob die Steuerungsleiste unten in der Komponente angezeigt werden soll.
Seitengröße	Legen Sie fest, wie viele Datensätze pro Seite angezeigt werden, wenn mehr Daten vorhanden sind, als auf einmal angezeigt werden können.
Wert 'Andere' anzeigen	Wenn diese Option ausgewählt ist, wird unten in einer Diagramm- oder Listenkomponente der Wert **Andere** angezeigt. Dieser entspricht der Gesamtzahl aller Datensätze, die auf der aktuellen Seite nicht angezeigt werden. Wenn Sie beispielsweise Seite 2 eines Datensatzes anzeigen, entspricht die Kategorie **Andere** der Summe der Werte von Seite 1 und allen Seiten nach Seite 2.
Legende anzeigen	Zeigen Sie unter oder rechts neben einem Kreisdiagramm eine Legende an.
Werte anzeigen	Schließen Sie die Werte für jedes Element eines Balkendiagramms ein.

Option	Beschreibung
Beschriftungen anzeigen	Schließen Sie für jeden Balken eines Balkendiagramms eine Beschriftung ein. Sie können festlegen, wie viele Zeichen maximal in einer Beschriftung angezeigt werden können. Wenn die Anzahl auf 0 festgelegt ist, gibt es kein Höchstlimit für die Beschriftung.
Durchschnittswerte der Basislinie anzeigen	Wählen Sie aus, ob die aktuellen Daten mit historischen Daten in einem Verteilungs- oder Balkendiagramm oder einer Messuhr verglichen werden sollen. Beim Anzeigen von Basisliniendaten können Sie zwei verschiedene Optionen verwenden: • **Automatischen Zeitbereich verwenden**: Wenn diese Option ausgewählt ist, werden die Basisliniendaten für den gleichen Zeitraum korreliert, der für die aktuelle Abfrage für die letzten fünf Intervalle verwendet wird. Wenn Sie beispielsweise den aktuellen Tag an einem Montag abfragen, werden die Basisliniendaten für die gleiche Zeit an den letzten fünf Montagen berechnet. Wenn für ein bestimmtes Intervall keine Daten vorhanden sind, werden weniger Intervalle verwendet. Anschließend wird der Durchschnitt der aus den einzelnen Intervallen gesammelten Werte ermittelt, um den aktuellen Basislinienwert zu berechnen. • **Bestimmten Zeitbereich verwenden**: Wenn Sie diesen Zeitbereich auswählen, können Sie eine Start- und Endzeit festlegen, die zum Berechnen eines Durchschnitts verwendet werden soll. Wenn Sie diese Option verwenden, wird der Durchschnitt für einen einzigen Zeitraum berechnet. Für Verteilungsberichte wird ein Durchschnitt in Form einer flachen Linie erzeugt. Basisliniendaten werden in Verteilungsdiagrammen als blaue Linie angezeigt. Die Linie ist flach, wenn die Option **Bestimmten Zeitbereich verwenden** ausgewählt ist oder nicht genug Daten vorhanden sind, um einen korrelierten Wert zu berechnen. Die Linie ist gekrümmt (in der Annahme, dass für jeden Zeitraum andere Werte angezeigt werden), wenn ein korrelierter Wert berechnet wird. Im Balkendiagramm wird für jeden Balken ein Pfeil am Basislinienpunkt angezeigt. Wenn der aktuelle Wert größer als der Basislinienwert ist, wird der Balken über der Basislinienmarkierung in Rot dargestellt. Wenn im Balkendiagramm der Schweregrad von Regeln angezeigt wird, ändert sich die Balkenfarbe für den Basislinienwert nicht. Mit einer weiteren Option können Sie einen Differenzwert festlegen, der zusammen mit den Basisliniendaten angezeigt werden soll. Der Differenzwert wird anhand des Basislinienwerts berechnet. Wenn beispielsweise der Basislinienwert 100 entspricht und die Differenz nach oben 20 % beträgt, wird der Randwert 120 berechnet. Wenn Sie diese Funktion aktivieren, wird der Differenzbereich für jeden Balken eines Balkendiagramms angezeigt. In einem Verteilungsdiagramm wird der Durchschnittswert der Basislinie berechnet und der Differenzbereich über und unter der Basislinie als schattierter Bereich angezeigt.
Geräteliste	Ziehen Sie Geräte in die Komponente **Netzwerktopologie** oder die Struktur **Logische Gerätegruppierungen**, und legen Sie sie dort ab.
Logische Gerätegruppierungen	Erstellen Sie Ordner, um die Geräte für die Komponente **Netzwerktopologie** zu gruppieren.
Hintergrund	Wählen Sie die Farbe für den Hintergrund der Ansicht aus. Mit **URL für Hintergrundbild** können Sie ein Bild importieren, um es als Hintergrund zu verwenden.

Hinzufügen von Geräten zur Netzwerktopologie-Komponente

Mit der Netzwerktopologie können Sie Ereignis- und Flussdaten aus den Geräten oder der Gerätestruktur abrufen und die entsprechenden Daten im gesamten Netzwerk anzeigen.

Bevor Sie beginnen

Sie müssen die Netzwerkerkennung ausführen, damit die Liste der Geräte angezeigt wird (siehe *Netzwerkerkennung*).

Außerdem können Sie eine benutzerdefinierte Ansicht erstellen, die Sie für Netzwerkerkennungsdaten verwenden können. Wenn Sie eine Ansicht für die Netzwerktopologie erstellt haben, müssen Sie diese anpassen, um die Ereignis- oder Flussinformationen anzuzeigen (siehe *Hinzufügen einer benutzerdefinierten Ansicht*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wenn Sie eine Ansicht hinzufügen oder bearbeiten, klicken Sie auf die Komponente **Netzwerktopologie für Ereignis**, ziehen Sie sie, und legen Sie sie an der gewünschten Stelle ab.

Im Bereich **Eigenschaften** werden die **Geräteliste** und die Struktur **Logische Gerätegruppierungen** angezeigt.

2 Wählen Sie in der **Geräteliste** oder **Ordnerliste** ein Gerät bzw. einen Ordner aus, und führen Sie einen der folgenden Schritte aus:

- Zum Hinzufügen des Geräts oder Ordners zur Komponente müssen Sie das Gerät bzw. den Ordner auf die Komponente ziehen und dort ablegen.
- Zum Hinzufügen des Geräts oder Ordners zu einer Gruppe in der Struktur **Logische Gerätegruppierungen** klicken Sie auf **Hinzufügen**, geben Sie einen Namen für den Ordner ein, und klicken Sie auf **OK**. Ziehen Sie dann das Gerät in den Ordner, und legen Sie es ab.

3 Ordnen Sie die Geräte an.

Geräte, die physisch mit dem System verbunden sind, sind mit einer geraden schwarzen Linie mit der Komponente verbunden. Blaue oder rote gekrümmte Linien weisen auf einen Datenpfad hin.

Gerätedetails in Netzwerktopologie-Komponenten

Sie können bestimmte Gerätedetails in einer **Netzwerktopologie**-Komponente anzeigen, wenn Sie auf ein Gerät doppelklicken. Auf diesem Bildschirm können Sie Informationen zu Schnittstellen und Endpunkten anzeigen, beispielsweise Port-Zusammenfassung, Gesamtanzahl der Geräte und Status von Geräten.

Option	Beschreibung
Port-Zusammenfassung für	Zeigt an, welchen Port Sie zurzeit anzeigen.
Insgesamt	Gibt die Gesamtanzahl der Geräte an.
Über dem Durchschnitt der Basislinie	Gibt die Anzahl der Geräte über dem aktuellen Durchschnitt der Basislinie an.
	Stellt eine Arbeitsstation dar.
	Gibt an, dass der Schnittstelle Warnungsdaten zugeordnet sind und dass die Daten den Durchschnitt der Basislinie unterschreiten.
	Gibt an, dass der Schnittstelle Warnungsdaten zugeordnet sind und dass die Daten den Durchschnitt der Basislinie überschreiten.

Option	Beschreibung
	Gibt an, dass der Schnittstelle keine Warnungsdaten zugeordnet sind.
	Gibt an, dass der Verwaltungsstatus Inaktiv entspricht (nicht nur in Bezug auf den Betrieb inaktiv).
	Stellt einen Router dar.
	Gibt an, dass der Switch-Port aktiv ist.
	Stellt ein unbekanntes Gerät dar.
	Stellt ein nicht verwaltetes Gerät dar.
	Gibt an, dass keine Kommunikation zwischen ESM und dem Gerät über SNMP, Netzwerkerkennung oder Ping möglich ist.

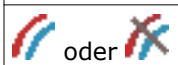
Komponenten-Symbolleiste

Die Komponenten-Symbolleiste befindet sich unten in jeder Komponente einer Ansicht und enthält verschiedene Aktionen, die Sie für die Daten in der Komponente ausführen können. Die verfügbaren Aktionen hängen vom Typ der Komponente ab.

Option	Beschreibung
	**Ereignisse als überprüft markieren**: Markieren Sie bestimmte Ereignisse, nachdem Sie sie überprüft haben. Dann können Sie mithilfe der Dropdown-Liste **Statusfilter für Ereignisse ändern** nur überprüfte Ereignisse oder nur nicht überprüfte Ereignisse anzeigen.
	**Ereignisse zu einem Fall oder zu Remedy zuweisen**: Weisen Sie Ereignisse einem Fall zu (siehe *Verwalten von Fällen*), oder senden Sie eine E-Mail-Nachricht an das Remedy-System (wenn dieses eingerichtet ist). Wenn Sie auf dieses Symbol klicken, können Sie folgende Optionen auswählen: • Neuen Fall erstellen • Ereignisse zu einem Fall hinzufügen • Ereignis an Remedy senden (siehe *Senden einer E-Mail an Remedy*)
	**URL zum Starten des Geräts**: Öffnen Sie die dem ausgewählten Ereignis zugeordnete URL, wenn Sie für das Gerät eine URL hinzugefügt haben (siehe *Hinzufügen einer URL*). Wenn Sie keine URL definiert haben, werden Sie aufgefordert, sie hinzuzufügen.
	**Host-Namen anzeigen** oder **Host-Namen ausblenden**: Sie können die Host-Namen, die den IP-Adressen in der Ansicht zugeordnet sind, anzeigen oder ausblenden (siehe *Verwalten von Host-Namen*).

Option	Beschreibung
Symbole für den Diagrammtyp	**Diagrammtyp ändern**: Ändern Sie den Typ des Diagramms, in dem die Daten angezeigt werden. Das Symbol für diese Funktion entspricht dem Komponentensymbol für den aktuellen Diagrammtyp.

Option	Beschreibung
	**Datendetails anzeigen** oder **Datendetails ausblenden**: Sie können Details zum ausgewählten Ereignis anzeigen oder ausblenden. Dieser Abschnitt enthält mehrere Registerkarten: • **Details**: Zeigt die verfügbaren Informationen zum ausgewählten Fluss oder Ereignis an. • **Erweiterte Details**: Zeigt Informationen zum Quell-Netzwerkgerät, Ziel-Netzwerkgerät und zu Abhilfen an. Wenn Sie über ausreichende Rechte zum Anzeigen der entsprechenden Datensätze verfügen, können Sie anhand der IDs nach Ereignissen oder Flüssen suchen, indem Sie auf das Lupensymbol rechts neben dem Feld **Ereignis-ID** oder **Fluss-ID** klicken. • **Geolocation**: Zeigt den Standort der Quelle und des Ziels des ausgewählten Ereignisses an. • **Beschreibung**: Zeigt den Namen, die Beschreibung und die Signatur oder Regel an, der bzw. die dem Ereignis zugeordnet ist. • **Hinweise**: Hier können Sie Hinweise zum Ereignis oder Fluss hinzufügen, die immer angezeigt werden, wenn Sie das jeweilige Element anzeigen. • **Paket**: Ruft den Inhalt des Pakets ab, von dem das ausgewählte Ereignis generiert wurde. Auf dieser Registerkarte können Sie die folgenden Funktionen ausführen: • Wählen Sie das Format zum Anzeigen des Pakets aus. • Rufen Sie die Paketdaten ab, indem Sie auf  klicken. • Speichern Sie das Paket auf dem Computer, indem Sie auf  klicken. Wenn es sich um eine Paketaufzeichnung (Packet Capture, PCAP) handelt (beispielsweise Nitro IPS-Ereignisse, ADM-Ereignisse, eStreamer-Ereignisse vom Empfänger), wird das Paket mit der Erweiterung .pcap gespeichert und kann in jedem PCAP-Anzeigeprogramm geöffnet werden. Anderenfalls wird das Paket als Textdatei gespeichert. • Legen Sie fest, dass das Paket automatisch abgerufen wird, wenn Sie auf ein Ereignis klicken. • Suchen Sie nach Informationen im Paket, indem Sie das Stichwort in das Feld **Text suchen** eingeben und auf  klicken.  Verwenden Sie im Feld **Text suchen** keine Sonderzeichen wie beispielsweise eckige oder runde Klammern. • **Quellereignisse**: Wenn ein Korrelations- oder Schwachstellenereignis ausgewählt ist, werden die

Option	Beschreibung
	Ereignisse angezeigt, durch die das zu generierende Ereignis verursacht wurde. • **ELM-Archiv**: Wenn Sie in das Feld **Text suchen** Text eingeben, werden auf dem ELM-Gerät archivierte Daten abgerufen. Wenn das Ereignis aggregiert ist, werden auf einem Empfänger oder ACE-Gerät bis zu 100 aggregierte Ereignisse angezeigt. • **Benutzerdefinierte Typen**: Wenn Sie benutzerdefinierte Typen definiert haben (siehe *Benutzerdefinierte Typfilter*), werden die Felder für benutzerdefinierte Typen und die Daten aus dem Ereignis angezeigt, die in diese Felder gehören. • **Informationen**: Zeigt Informationen wie beispielsweise Gerätename, IP-Adresse, Betriebssystem und Geräteversion, Systembeschreibung, Kontaktperson für das System und physischer Standort des Systems an. • **Schnittstellen**: Zeigt Port-Name, Port-Geschwindigkeit, VLAN, Verwaltungsstatus und Betriebsstatus an. • **Nachbarn**: Zeigt spezifische Informationen zu den Nachbargeräten an, beispielsweise lokale Schnittstelle, Nachbargerät und Nachbarschnittstelle.
	**Intervallzeitraum ändern und Intervallrate ändern**: Legen Sie fest, wie oft die Daten im Diagramm aktualisiert werden sollen.
	**Rate festlegen**: Wählen Sie die Rate für die angezeigten Daten aus (keine, pro Sekunde, pro Minute, pro Stunde, pro Tag, pro Woche, pro Monat).
	**IP-Adresse** : Zeigen Sie die Quell- und Zielereignisse oder -flüsse für eine bestimmte IP-Adresse an. Geben Sie die Adresse in das Feld ein, oder wählen Sie eine zuvor verwendete Adresse aus, und klicken Sie auf das Symbol **Aktualisieren**  .
	**Geolocation-Optionen**: Markieren Sie mit der **STRG**-Taste und der **UMSCHALTTASTE** wahlweise Ort, Bundesland, Land und Weltregion, vergrößern und verkleinern Sie die Anzeige, und wählen Sie Standorte aus.
	**Seite ändern**: Navigieren Sie durch Daten auf mehreren Seiten.
	**Statusfilter für Ereignisse ändern**: Wählen Sie den Typ der Ereignisse oder Flüsse aus, die in der Analyseliste angezeigt werden sollen. Sie können alle Ereignisse, nur überprüfte Ereignisse, nur nicht überprüfte Ereignisse, behobene Ereignisse, alle Flüsse, nur offene Flüsse oder nur geschlossene Flüsse anzeigen.
	Verlaufschaltflächen: Führen Sie in den an der Ansicht vorgenommenen Änderungen einen Bildlauf vorwärts und rückwärts aus.
	**Datenpfade anzeigen** oder **Datenpfade ausblenden**: Sie können die Verbindungslinie zwischen zwei Geräten mit Ereignis- oder Flussdatenverbindungen ausblenden oder anzeigen.
	**Text ausblenden**: Sie können die Beschriftungen des Geräts in der Netzwerktopologie-Ansicht ausblenden oder anzeigen.

Senden einer E-Mail an Remedy

Wenn Sie ein Remedy-System einrichten, können Sie eine E-Mail-Nachricht senden, um das System über ein Ereignis zu benachrichtigen, bei dem eine Abhilfemaßnahme erforderlich ist. Wenn Sie diesem Prozess folgen, erhalten Sie eine Remedy-Fallnummer, die Sie zum Ereignisdatensatz hinzufügen.

Ein Remedy-System wird vom Benutzer eingerichtet und ist nicht mit McAfee Nitro IPS verbunden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Heben Sie in einer Ereignisansicht das Ereignis hervor, bei dem eine Abhilfemaßnahme erforderlich ist.

2 Klicken Sie auf das Symbol **Ereignisse zu einem Fall oder zu Remedy zuweisen**  , und wählen Sie dann **Ereignis an Remedy senden** aus.

3 Fügen Sie **Präfix**, **Stichwort** und **Unternehmensbenutzer-ID** hinzu.

4 (Optional) Fügen Sie unter **Details** Informationen hinzu. Der Abschnitt enthält vom System generierte Informationen zu dem Ereignis.

5 Klicken Sie auf **Senden**.

Menüoptionen für Komponenten

Die meisten Komponenten einer Ansicht verfügen über ein Menü  , in dem die für die jeweilige Komponente verfügbaren Optionen aufgeführt sind. Die folgende Tabelle enthält alle verfügbaren Elemente.

Option		Beschreibung
Aufgliedern (Ereignis, Fluss, Ressource)		Zeigen Sie weitere Details für den in den Aufgliederungslisten ausgewählten Datentyp an. Die Details werden in einer neuen Ansicht angezeigt.
Zusammenfassen oder **Zusammenfassen nach**		Zeigen Sie weitere Ereignis- oder Flussdaten an, die teilweise die gleichen Merkmale aufweisen wie die ausgewählten Ereignisse. Wenn Sie beispielsweise ein Port-Scan-Ereignis auf dem Analysebildschirm anzeigen und weitere vom gleichen Angreifer generierte Ereignisse sehen möchten, klicken Sie auf das Ereignis, wählen Sie **Zusammenfassen nach** aus, und klicken Sie dann auf **Quell-IP**.
Aggregationseinstellungen ändern		Erstellen Sie für eine einzelne Regel eine Ausnahme von den allgemeinen Aggregationseinstellungen (siehe *Hinzufügen von Ausnahmen für Einstellungen für die Ereignisaggregation*).
Aktionen	**Neue Watchlist erstellen**	Wählen Sie in einer Ansicht Ereignisse aus, und fügen Sie sie zu einer neuen Watchlist hinzu (siehe *Watchlists*).
	An Überwachungsliste anfügen	Wählen Sie in einer Ansicht Ereignisse aus, und fügen Sie sie zu einer vorhandenen Überwachungsliste hinzu.
	Neuen Alarm erstellen	Wählen Sie in einer Ansicht Ereignisse aus, und erstellen Sie einen Alarm, der auf den Werten der Ereignisse basiert (siehe *Erstellen eines Alarms*).
	MVM-Scan ausführen	Initiieren Sie einen McAfee Vulnerability Manager-Scan, wenn das System ein McAfee Vulnerability Manager-Gerät enthält.
	ePO starten	Öffnen Sie die ePolicy Orchestrator-Benutzeroberfläche (siehe *Starten von ePolicy Orchestrator*).

Option	Beschreibung
Ausführungsverlauf für TIE	Wählen Sie ein TIE-Ereignis aus, und öffnen Sie die Seite **Ausführungsverlauf für TIE**, um die IP-Adressen anzuzeigen, über die versucht wurde, die ausgewählte Datei auszuführen. Auf dieser Seite können Sie eine neue Watchlist erstellen, eine Datei an eine Watchlist anfügen, einen neuen Alarm erstellen, eine Datei in die Blacklist aufnehmen, eine Datei im CSV-Format exportieren oder ePolicy Orchestrator-Tags zur Datei hinzufügen.
Regel anzeigen	Zeigen Sie die Regel an, von der das Ereignis generiert wurde.
Details zur IP-Adresse	Hiermit suchen Sie Informationen zu einer Quell- oder Ziel-IP-Adresse oder einem Quell- oder Zielport. Sie können Bedrohungsdetails und die Ergebnisse der WHOIS-Suche für die ausgewählte IP-Adresse anzeigen.
ASN-Suche	Rufen Sie mit der ASN-ID einen WHOIS-Datensatz ab.
Referenz durchsuchen	Öffnen Sie den Standard-Web-Browser, und stellen Sie eine Verbindung mit der online verfügbaren McAfee-Signaturdatenbank her. Diese enthält Informationen zu der Signatur, von der das ausgewählte Ereignis generiert wurde.
Remedy-Fall-ID festlegen	Fügen Sie zum Ereignisdatensatz zu Referenzzwecken die Remedy-Fall-ID hinzu, die Sie beim Senden einer Ereignis-E-Mail an das Remedy-System erhalten haben (siehe *Hinzufügen einer Remedy-Fall-ID zu einem Ereignisdatensatz*).
Blacklist	Fügen Sie die IP-Adresse aus dem ausgewählten Ereignis zur Blacklist hinzu. Wenn Sie diese Option auswählen, wird der **Blacklist-Editor** geöffnet, in dem das Feld für die IP-Adresse mit den Daten aus dem ausgewählten Ereignis ausgefüllt ist (siehe *I Blacklist für IPS oder virtuelles Gerät*).
ELM durchsuchen	Führen Sie auf dem ELM-Gerät eine Suche nach Informationen zum ausgewählten Ereignis aus. Daraufhin wird die Seite **Erweiterte ELM-Suche** geöffnet, die mit den ausgewählten Daten ausgefüllt ist (siehe *Ausführen einer erweiterten ELM-Suche*).
VLAN ändern	Ändern Sie das VLAN für ausgewählte Geräte. Sie können 1 bis 12 Geräte auswählen.
Ports deaktivieren oder Ports aktivieren	Wählen Sie eine Schnittstelle bzw. einen Endpunkt oder mehrere Schnittstellen bzw. Endpunkte aus. Abhängig von der Auswahl wird die Option zum Deaktivieren oder zum Aktivieren angezeigt. Wenn Sie beispielsweise fünf Schnittstellen auswählen, wobei eine aktiviert ist und die anderen vier deaktiviert sind, können Sie den Port nur deaktivieren. Wenn Sie jedoch einen deaktivierten Port auswählen, ist die Option **Ports aktivieren** verfügbar.
Ereignisse anzeigen oder Flüsse anzeigen	Zeigen Sie die von einem Fluss generierten Ereignisse oder die von einem Ereignis generierten Flüsse an.
Exportieren	Exportieren Sie eine Ansichtskomponente im PDF-Format, Textformat, CSV- oder HTML-Format (siehe *Exportieren einer Komponente*).
Löschen	Löschen Sie Ereignisse oder Flüsse aus der Datenbank. Sie müssen einer Gruppe mit Ereignisberechtigungen angehören und können nur die zurzeit ausgewählten Datensätze, die aktuelle Seite mit Daten oder eine maximale Anzahl von Seiten ab Seite 1 löschen.
Als überprüft markieren	Kennzeichnen Sie Ereignisse als überprüft. Sie können alle Datensätze im Ergebnissatz, die aktuelle Seite oder ausgewählte Datensätze markieren.

Option	Beschreibung
Benutzerdefinierte Firewall-Regel erstellen	Erstellen Sie eine benutzerdefinierte Firewall-Regel, die auf den Eigenschaften des ausgewählten Ereignisses oder Flusses basiert. Wenn Sie auf **Benutzerdefinierte Firewall-Regel erstellen** klicken, wird die Seite **Neue Regel** geöffnet (siehe *Hinzufügen benutzerdefinierter ADM-Regeln, Datenbankregeln oder Korrelationsregeln*).
Benutzerdefinierte Regel erstellen	Erstellen Sie eine benutzerdefinierte Regel, und verwenden Sie dabei als Ausgangspunkt die Signatur, von der eine bestimmte Warnung ausgelöst wurde. Diese Option ist verfügbar, wenn Sie durch Standardregeln (Nicht-Firewall-Regeln) generierte Warnungen auswählen. Wenn Sie auf **Benutzerdefinierte Regel erstellen** klicken, wird die Seite **Neue Regel** geöffnet (siehe *Hinzufügen benutzerdefinierter ADM-Regeln, Datenbankregeln oder Korrelationsregeln*).

Ausführen einer WHOIS- oder ASN-Suche

Sie können in einer Tabellenkomponente eine WHOIS-Suche ausführen, um Informationen zu einer Quell- oder Ziel-IP-Adresse zu finden. Mit der für jede ASN-Abfrage in einem Balkendiagramm und für jeden Flussdatensatz in einer Tabellenkomponente mit ASN-Daten verfügbaren **ASN-Suche** können Sie anhand der ASN-ID einen WHOIS-Datensatz abrufen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie eine IP-Adresse oder einen Flussdatensatz mit ASN-Daten in einer Tabellenkomponente oder eine ASN-Abfrageleiste in einer Balkendiagrammkomponente aus.

2 Klicken Sie auf das Menü  , und wählen Sie dann **Details zur IP-Adresse** oder **ASN-Suche** aus.

3 So suchen Sie eine andere IP-Adresse oder ID:

- Wählen Sie auf der Registerkarte **WHOIS** in der Dropdown-Liste eine IP-Adresse aus, und geben Sie den Host-Namen ein.
- Geben Sie auf der Seite **ASN-Suche** die Zahlen ein, oder wählen Sie in der Dropdown-Liste eine Zahl aus.

Hinzufügen einer Remedy-Fall-ID zu einem Ereignisdatensatz

Wenn Sie eine Ereignis-E-Mail an das Remedy-System senden, erhalten Sie eine Fall-ID. Diese können Sie zu Referenzzwecken zum Ereignisdatensatz hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Heben Sie in der Ansicht **Ereignisanalyse** das Ereignis hervor, und klicken Sie dann auf das Menü  .

2 Wählen Sie **Remedy-Fall-ID festlegen** aus, geben Sie die Nummer ein, und klicken Sie auf **OK**.

Exportieren einer Komponente

Sie können die Daten einer ESM-Ansichtskomponente exportieren. Diagrammkomponenten können im Textformat oder PDF-Format exportiert werden, Tabellenkomponenten können im CSV-Format (durch Komma getrennte Werte) oder im HTML-Format exportiert werden.

Wenn Sie die aktuelle Seite einer Diagramm-, Verteilungs- oder Tabellenkomponente in einer Ansicht exportieren, entsprechen die exportierten Daten genau denen, die beim Initiieren des Exports angezeigt werden. Wenn Sie mehrere Seiten exportieren, wird die Abfrage beim Exportieren der Daten erneut ausgeführt und kann sich daher von dem unterscheiden, was in der Komponente angezeigt wird.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in einer Ansicht auf das Menü  der zu exportierenden Komponente und dann auf **Exportieren**.

2 Wählen Sie eines der folgenden Formate aus:

- **Text**: Exportieren Sie die Daten im Textformat.
- **PDF**: Exportieren Sie die Daten zusammen mit einem Bild.
- **Bild in PDF**: Exportieren Sie nur das Bild.
- **CSV**: Exportieren Sie eine Liste im durch Komma getrennten Format.
- **HTML**: Exportieren Sie die Daten in einer Tabelle.

3 Geben Sie auf der Seite **Exportieren** die Daten an, die Sie exportieren möchten.

- Wenn Sie **Text** oder **PDF** ausgewählt haben, können Sie die aktuelle Seite mit Daten oder eine maximale Seitenanzahl beginnend mit Seite 1 exportieren.
- Wenn Sie **Bild in PDF** ausgewählt haben, wird das Bild generiert.
- Wenn Sie **CSV** oder **HTML** ausgewählt haben, können Sie nur die ausgewählten Elemente, nur die aktuelle Seite mit Daten oder eine maximale Seitenanzahl beginnend mit Seite 1 exportieren.

4 Klicken Sie auf **OK**.

Die Exportdatei wird generiert, und Sie werden aufgefordert, die sich ergebende Datei herunterzuladen.

Arbeiten mit dem Abfragen-Assistenten

In den einzelnen Berichten oder Ansichten auf dem ESM-Gerät werden Daten basierend auf den Abfrageeinstellungen für die einzelnen Komponenten gesammelt.

Beim Hinzufügen oder Bearbeiten einer Ansicht oder eines Berichts definieren Sie die Abfrageeinstellungen für die einzelnen Komponenten im **Abfragen-Assistenten**, indem Sie den Abfragetyp, die Abfrage, die einzuschließenden Felder und die zu verwendenden Filter auswählen. Alle Abfragen im System (vordefinierte und benutzerdefinierte Abfragen) werden im Assistenten aufgeführt, sodass Sie die Daten auswählen können, die von der Komponente gesammelt werden sollen. Außerdem können Sie Abfragen bearbeiten oder entfernen und eine vorhandene Abfrage kopieren, um sie als Vorlage beim Einrichten einer neuen Abfrage zu verwenden.

Verwalten von Abfragen

Im Lieferumfang des ESM-Geräts sind vordefinierte Abfragen enthalten, die Sie im **Abfragen-Assistenten** auswählen können, wenn Sie einen Bericht oder eine Ansicht hinzufügen oder bearbeiten. Sie können einige der Einstellungen für diese Abfragen bearbeiten und benutzerdefinierte Abfragen hinzufügen und entfernen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Führen Sie einen der folgenden Schritte aus, um auf den **Abfragen-Assistenten** zuzugreifen.

Aufgabe	Vorgehensweise
Hinzufügen einer neuen Ansicht	1 Klicken Sie auf der Ansichtssymbolleiste auf das Symbol **Neue Ansicht erstellen**  . 2 Ziehen Sie eine Komponente aus der **Symbolleiste zum Bearbeiten von Ansichten** in den Ansichtsbereich, und legen Sie sie dort ab. Der **Abfragen-Assistent** wird geöffnet.
Bearbeiten einer vorhandenen Ansicht	1 Wählen Sie die zu bearbeitende Ansicht aus. 2 Klicken Sie auf der Ansichtssymbolleiste auf das Symbol **Aktuelle Ansicht bearbeiten**  . 3 Klicken Sie auf die zu bearbeitende Komponente. 4 Klicken Sie im Bereich **Eigenschaften** auf **Abfrage bearbeiten**. Die zweite Seite des **Abfragen-Assistenten** wird geöffnet.
Entwerfen des Layouts für einen neuen Bericht	1 Klicken Sie in **Systemeigenschaften** auf **Berichte**. 2 Klicken Sie auf **Hinzufügen**. 3 Klicken Sie in Abschnitt 5 der Seite **Bericht hinzufügen** auf **Hinzufügen**. 4 Ziehen Sie eine Komponente in den Abschnitt für das Berichtslayout, und legen Sie sie dort ab. Der **Abfragen-Assistent** wird geöffnet.
Bearbeiten des Layouts eines vorhandenen Berichts	1 Klicken Sie in **Systemeigenschaften** auf **Berichte**. 2 Wählen Sie den zu bearbeitenden Bericht aus, und klicken Sie dann auf **Bearbeiten**. 3 Wählen Sie in Abschnitt 5 der Seite **Bericht bearbeiten** ein vorhandenes Layout aus, und klicken Sie dann auf **Bearbeiten**. 4 Klicken Sie im Abschnitt mit dem Berichtslayout auf die Komponente und dann im Abschnitt **Eigenschaften** auf **Abfrage bearbeiten**. Die zweite Seite des **Abfragen-Assistenten** wird geöffnet.

2 Führen Sie im **Abfragen-Assistenten** einen der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Hinzufügen einer neuen Abfrage	1 Wählen Sie die Abfrage aus, die Sie als Vorlage verwenden möchten, und klicken Sie dann auf **Kopieren**. 2 Geben Sie den Namen für die neue Abfrage ein, und klicken Sie dann auf **OK**. 3 Klicken Sie in der Liste der Abfragen auf die gerade hinzugefügte Abfrage und dann auf **Weiter**. 4 Ändern Sie auf der zweiten Seite des Assistenten die Einstellungen, indem Sie auf die Schaltflächen klicken.
Bearbeiten einer benutzerdefinierten Abfrage	1 Wählen Sie die zu bearbeitende benutzerdefinierte Abfrage aus, und klicken Sie dann auf **Bearbeiten**. 2 Ändern Sie auf der zweiten Seite des Assistenten die Einstellungen, indem Sie auf die Schaltflächen klicken.
Entfernen einer benutzerdefinierten Abfrage	Wählen Sie die zu entfernende benutzerdefinierte Abfrage aus, und klicken Sie dann auf **Entfernen**.

3 Klicken Sie auf **Fertig stellen**.

Binden von Komponenten

Wenn eine Ansichtskomponente über eine Datenbindung mit einer anderen Komponente verknüpft ist, wird die Ansicht interaktiv.

Wenn Sie mindestens ein Element in der übergeordneten Komponente auswählen, werden die in der untergeordneten Komponente angezeigten Elemente so geändert, als hätten Sie eine Aufgliederung nach weiteren Details ausgeführt. Wenn Sie beispielsweise eine Quell-IP-Komponente eines übergeordneten Balkendiagramms an eine Ziel-IP-Komponente eines untergeordneten Balkendiagramms binden und in der übergeordneten Komponente eine Auswahl vornehmen, wird die Abfrage der untergeordneten Komponente mit der ausgewählten Quell-IP als Filter ausgeführt. Wenn Sie die Auswahl in der übergeordneten Komponente ändern, werden die Daten in der untergeordneten Komponente aktualisiert.

Mit der Datenbindung können Sie nur jeweils ein Feld an ein anderes binden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Erstellen Sie die übergeordneten und untergeordneten Komponenten, und wählen Sie dann die untergeordnete Komponente aus.

2 Klicken Sie im Bereich **Eigenschaften** auf **Abfrage bearbeiten** | **Filter**.

Daraufhin wird die Seite **Abfragefilter** geöffnet, auf der die übergeordneten und untergeordneten Abfragen aktiviert sind.

3 Wählen Sie in der Dropdown-Liste für die untergeordnete Abfrage die Option **Binden an** aus.

4 Klicken Sie auf **OK** und dann auf **Fertig stellen**.

Vergleichen von Werten

Verteilungsdiagramme haben eine Option, mit der Sie das aktuelle Diagramm mit einer zusätzlichen Variable überlagern können.

Auf diese Weise können Sie zwei Werte vergleichen, um leicht die Beziehungen beispielsweise zwischen der Gesamtzahl der Ereignisse und dem durchschnittlichen Schweregrad anzuzeigen. Mit dieser Funktion erhalten Sie auf einen Blick wertvolle Datenvergleiche im Zeitverlauf. Die Funktion ist auch beim Erstellen umfangreicher Ansichten hilfreich, um Platz auf dem Bildschirm zu sparen, indem Sie die Ergebnisse in einem einzigen Verteilungsdiagramm kombinieren.

Der Vergleich ist auf den Typ der ausgewählten Abfrage begrenzt. Wenn beispielsweise eine Ereignisabfrage ausgewählt ist, können Sie nur einen Vergleich mit den Feldern aus der Ereignistabelle durchführen, nicht mit der Fluss-, Ressourcen- und Schwachstellentabelle.

Wenn Sie die Abfrageparameter auf das Verteilungsdiagramm anwenden, wird die Abfrage normal ausgeführt. Wenn das Vergleichsfeld aktiviert ist, wird gleichzeitig eine sekundäre Abfrage für die Daten ausgeführt. In der Verteilungskomponente werden die Daten für beide Datensätze im gleichen Diagramm, jedoch mit zwei getrennten vertikalen Achsen angezeigt. Wenn Sie den Diagrammtyp ändern (rechte untere Ecke der Komponente), werden weiterhin beide Datensätze angezeigt.

Vergleichen von Diagrammwerten

Sie können die Daten in einem Verteilungsdiagramm mit einer ausgewählten Variablen vergleichen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie das Symbol **Neue Ansicht erstellen**  oder **Aktuelle Ansicht bearbeiten**  aus.
2. Klicken Sie auf das Symbol **Verteilung**  , ziehen Sie es in die Ansicht, und legen Sie es dort ab, um den **Abfragen-Assistenten** zu öffnen.
3. Wählen Sie den Abfragetyp und die Abfrage aus, und klicken Sie dann auf **Weiter**.
4. Klicken Sie auf **Vergleichen**, und wählen Sie dann das Feld aus, das Sie mit der ausgewählten Abfrage vergleichen möchten.
5. Klicken Sie auf **OK** und dann auf **Fertig stellen**.
6. Verschieben Sie die Komponente an die richtige Position in der Ansicht, und führen Sie dann die folgenden Schritte aus:
   - Wenn Sie die Komponente zu einer vorhandenen Ansicht hinzufügen, klicken Sie auf **Speichern**.
   - Wenn Sie eine neue Ansicht erstellen, klicken Sie auf **Speichern unter**, und fügen Sie den Namen für die Ansicht hinzu.

Einrichten der gestapelten Verteilung für Ansichten und Berichte

Richten Sie die Verteilungskomponente in einer Ansicht oder einem Bericht so ein, dass Sie die Verteilung der Ereignisse im Zusammenhang mit einem bestimmten Feld sehen können.

Sie können beim Hinzufügen der Komponente zu einer Ansicht oder einem Bericht das Feld auswählen, nach dem gestapelt werden soll. Wenn Sie auf die Ansicht zugreifen, können Sie die Einstellungen ändern, das Zeitintervall festlegen und Diagrammtyp und Details festlegen.

Die Funktionen **Stapeln** und **Vergleichen** können nicht in der gleichen Abfrage verwendet werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Ziehen Sie die **Verteilungs**komponente in einer Ansicht oder einem Bericht an die gewünschte Stelle, und legen Sie sie dort ab (siehe *Hinzufügen einer benutzerdefinierten Ansicht* oder *Hinzufügen eines Berichtslayouts*). Wählen Sie dann den Typ der Abfrage aus.

> Stapeln ist für Verteilungsabfragen vom Typ **Erfassungsrate** oder **Durchschnitt** (beispielsweise **Durchschnitt für Schweregrad pro Warnung** oder **Durchschnitt für Dauer pro Fluss**) nicht verfügbar.

2 Klicken Sie auf der zweiten Seite des **Abfragen-Assistenten** auf **Stapeln**, und wählen Sie dann die Optionen aus.

3 Klicken Sie auf der Seite **Stapeloptionen** auf **OK** und im **Abfragen-Assistenten** auf **Fertig stellen**.

Die Ansicht wird hinzugefügt. Sie können die Einstellungen ändern und Zeitintervall und Diagrammtyp festlegen, indem Sie auf das Symbol **Diagrammoptionen** klicken.

Ansichten verwalten

Das Verwalten von Ansichten ist eine Möglichkeit, schnell mehrere Ansichten gleichzeitig zu kopieren, importieren oder exportieren. Außerdem können Sie die Ansichten auswählen, die in der Liste der Ansichten enthalten sein sollen, und bestimmten Benutzern oder Gruppen Zugriffsberechtigungen für einzelne Ansichten zuweisen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ESM-Konsole auf das Symbol **Ansichten verwalten**.

2 Führen Sie eine oder mehrere der verfügbaren Optionen aus, und klicken Sie dann auf **OK**.

Untersuchen der umliegenden Ereignisse eines Ereignisses

In der Ansicht **Ereignisanalyse** können Sie nach Ereignissen suchen, die innerhalb des ausgewählten Zeitraums vor und nach dem Ereignis mit mindestens einem der Felder im Ereignis übereinstimmen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ESM-Konsole auf die Liste der Ansichten, und wählen Sie dann Folgendes aus: **Ereignisansichten** | **Ereignisanalyse**.

2 Klicken Sie auf an Ereignis, klicken Sie auf das Menüsymbol und dann auf **Umliegende Ereignisse untersuchen**.

3 Wählen Sie aus, wie viele Minuten vor und nach dem Zeitpunkt des Ereignisses vom System nach einer Übereinstimmung durchsucht werden sollen.

4 Klicken Sie auf **Filter auswählen**, wählen Sie das Feld aus, für das eine Übereinstimmung gesucht werden soll, und geben Sie dann den Wert ein.

Die Ergebnisse werden in der Ansicht **Ergebnisse der Untersuchung der umliegenden Ereignisse** angezeigt.

Wenn Sie diese Ansicht verlassen und später zurückkehren möchten, klicken Sie im Menü **Ereignisanalyse** auf **Letzte Untersuchung der umliegenden Ereignisse**.

Anzeigen der Details zur IP-Adresse eines Ereignisses

Wenn Sie über eine McAfee® Global Threat Intelligence™ (McAfee GTI)-Lizenz von McAfee verfügen, können Sie beim Ausführen einer Suche nach **Details zur IP-Adresse** auf die neue Registerkarte **Bedrohungsdetails** zugreifen. Wenn Sie diese Option auswählen, werden Details zur IP-Adresse zurückgegeben, unter anderem der Risikoschweregrad und Geolocation-Daten.

Bevor Sie beginnen

Erwerben Sie eine McAfee GTI-Lizenz (siehe *McAfee GTIWatchlist*).

Wenn Ihre McAfee GTI-Lizenz abgelaufen ist, wenden Sie sich an einen McAfee-Vertriebsingenieur oder an den McAfee-Support.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der ESM-Konsole eine Ansicht aus, die eine Tabellenkomponente enthält, beispielsweise **Ereignisansichten** | **Ereignisanalyse**.

2 Klicken Sie auf eine IP-Adresse, auf das Menüsymbol  in einer beliebigen Komponente mit einer IP-Adresse und dann auf **Details zur IP-Adresse**.

Auf der Registerkarte **Bedrohungsdetails** werden die Daten für die ausgewählte IP-Adresse aufgeführt. Sie können die Daten in die Zwischenablage des Systems kopieren.

Durch die Option **Details zur IP-Adresse** wurde die Option **WHOIS-Suche** im Kontextmenü ersetzt. Die Seite **Details zur IP-Adresse** enthält jedoch die Registerkarte **WHOIS-Suche**, auf der diese Informationen angezeigt werden.

Ändern der Standardansicht

Die Ansicht **Standardzusammenfassung** wird standardmäßig im Ansichtsbereich angezeigt, wenn Sie sich erstmals bei der ESM-Konsole anmelden. Sie können diese Standardansicht in eine beliebige vordefinierte oder benutzerdefinierte Ansicht des ESM-Geräts ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf der Navigationsleiste der ESM-Konsole auf **Optionen**, und wählen Sie dann **Ansichten** aus.

2 Wählen Sie in der Dropdown-Liste **Standardsystemansicht** die neue Standardansicht aus, und klicken Sie dann auf **OK**.

Filtern von Ansichten

Im Filterbereich der Hauptkonsole von ESM können Sie Filter einrichten, die auf Ansichten angewendet werden können. Alle auf eine Ansicht angewendeten Filter werden für die nächste geöffnete Ansicht übernommen.

Wenn Sie sich erstmals bei ESM anmelden, enthält der Bereich mit den Standardfiltern die Filterfelder **Quellbenutzer**, **Zielbenutzer**, **Quell-IP** und **Ziel-IP**. Sie können Filterfelder hinzufügen und löschen, Filtersätze speichern, den Standardsatz ändern, alle Filter verwalten und den Manager für die Normalisierung von Zeichenfolgen starten.

Rechts oben im Ansichtsbereich wird ein orangefarbiges Trichtersymbol angezeigt. Daran erkennen Sie, ob Filter auf die Ansicht angewendet wurden. Wenn Sie auf das orangefarbige Symbol klicken, werden alle Filter gelöscht, und die Abfrage wird erneut ausgeführt.

An allen Stellen, an denen Sie durch Komma getrennte Filterwerte (beispielsweise Variablen, globale Filter, lokale Filter, normalisierte Zeichenfolgen oder Berichtsfilter) verwenden, die nicht Teil einer Watchlist sind, müssen Sie Anführungszeichen verwenden. Für den Wert `Smith,John` müssen Sie `"Smith,John"` eingeben. Wenn der Wert Anführungszeichen enthält, müssen Sie die Anführungszeichen wiederum in Anführungszeichen einschließen. Für den Wert `Smith,"Boy"John` müssen Sie `"Smith,""Boy""John"` eingeben.

Sie können `contains`-Filter und Filter für `reguläre Ausdrücke` verwenden (siehe **Beschreibung der contains-Filter und Filter für reguläre Ausdrücke**).

Filtern einer Ansicht

Mithilfe von Filtern können Sie Details zu ausgewählten Elementen in einer Ansicht anzeigen. Wenn Sie Filter eingeben und die Ansicht aktualisieren, entsprechen die Daten in der Ansicht den hinzugefügten Filtern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der ESM-Konsole auf die Dropdown-Liste der Ansichten, und wählen Sie dann die zu filternde Ansicht aus.
2. Füllen Sie im Bereich **Filter** die Felder mit den Daten aus, nach denen Sie filtern möchten. Sie haben folgende Möglichkeiten:
   - Geben Sie die Filterinformationen in das entsprechende Feld ein. Wenn Sie beispielsweise die aktuelle Ansicht so filtern möchten, dass nur Daten mit der Quell-IP-Adresse 161.122.15.13 angezeigt werden, geben Sie die IP-Adresse in das Feld **Quell-IP** ein.
   - Geben Sie einen `contains`-Filter oder einen Filter für `reguläre Ausdrücke` ein (siehe *Beschreibung der `contains`-Filter und Filter für `reguläre Ausdrücke`*).
   - Klicken Sie neben dem Feld auf das Symbol **Filterliste anzeigen**  , und wählen Sie die Variablen bzw. die Watchlists aus, nach denen Sie filtern möchten.
   - Wählen Sie in der Ansicht die Daten aus, die Sie als Filter verwenden möchten, und klicken Sie dann im Bereich **Filter** auf das entsprechende Feld. Wenn das Feld leer ist, wird es automatisch mit den ausgewählten Daten ausgefüllt.

     Für **Durchschnitt für Schweregrad** können Sie mit einem Doppelpunkt (:) einen Bereich eingeben. Beispielsweise entspricht 60:80 dem Schweregradbereich von 60 bis 80.
3. Führen Sie eine oder mehrere der folgenden Aktionen aus:

Aufgabe	Vorgehensweise
Anzeigen von Daten, die mit mehreren Filtern übereinstimmen	Geben Sie die Werte in die einzelnen Felder ein.
Anzeigen von Daten, die mit einigen Filterwerten übereinstimmen, und Ausschließen anderer Daten	1 Geben Sie die Filterwerte ein, die Sie ein- bzw. ausschließen möchten. 2 Klicken Sie neben den auszuschließenden Feldern auf das Symbol **NICHT** !.
Anzeigen von Daten, die mit Filtern für reguläre Ausdrücke oder ODER-Filtern übereinstimmen	1 Geben Sie die Filterwerte in die Felder für reguläre Ausdrücke und für **ODER** ein. 2 Klicken Sie auf das Symbol **ODER** neben den Feldern mit den **ODER**-Werten. Die Ansicht enthält die Daten, die mit den Werten in den nicht mit **ODER** markierten Feldern und mit einem der Werte in den mit **ODER** markierten Feldern übereinstimmen. Sie müssen mindestens zwei Felder mit **ODER** markieren, damit dieser Filter funktioniert.
Ignorieren der Groß-/Kleinschreibung der Filterwerte	Klicken Sie neben dem entsprechenden Filterfeld auf das Symbol **Groß-/Kleinschreibung ignorieren** Aa.
Ersetzen normalisierter Zeichenfolgen durch ihre Aliasse	Klicken Sie neben dem entsprechenden Filterfeld auf das Symbol Zeichenfolgennormalisierung .

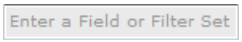
4 Klicken Sie auf das Symbol **Abfrage ausführen** .

Die Ansicht wird aktualisiert, und die Datensätze, die den eingegebenen Werten entsprechen, werden in der Ansicht angezeigt. Rechts oben im Ansichtsbereich wird ein orangefarbiges Filtersymbol angezeigt. Daran erkennen Sie, dass die Daten in der Ansicht gefiltert sind. Wenn Sie auf das Symbol klicken, werden die Filter gelöscht, und in der Ansicht werden alle Daten angezeigt.

Bereich Filter

Der Filterbereich enthält Optionen, mit denen Sie Filter für die Ansichten festlegen können.

Symbol	Bedeutung	Beschreibung
	Hinweise	Wenn Sie in ein Filterfeld klicken, wird eine QuickInfo angezeigt.
	Manager für die Normalisierung von Zeichenfolgen starten	Mit dieser Option können Sie nach einer Zeichenfolge und deren Aliassen filtern (siehe *Zeichenfolgennormalisierung*).
	Abfrage ausführen	Mit dieser Option wenden Sie die aktuellen Filter auf die Ansicht an. Sie müssen auf dieses Symbol klicken, wenn Sie einen Filterwert ändern und diesen auf die aktuelle Ansicht anwenden möchten.
	Alle löschen	Mit dieser Option löschen Sie alle Filter aus dem Filterbereich.

Symbol	Bedeutung	Beschreibung
	**Optionen für Filtersätze**	Wählen Sie eine Aktion aus, die für die Filtersätze ausgeführt werden soll. • **Als Standard festlegen**: Speichert die Filterwerte, die Sie als Standard eingegeben haben. Diese Filter werden automatisch angewendet, wenn Sie sich anmelden. • **Standard wiederherstellen**: Setzt die Filter auf die Standardwerte zurück, sodass Sie die Abfrage mit dem Standardfiltersatz ausführen können. • **Ausgefüllte Filter speichern**: Speichert den aktuellen Filtersatz und fügt ihn der Liste der verfügbaren Filter hinzu, in der Sie ihn beim Hinzufügen eines Filters auswählen können. Geben Sie einen Namen für den Satz ein, und wählen Sie dann den Ordner aus, indem der Satz gespeichert werden soll. • **Filter verwalten**: Öffnet die Seite **Verwalten von Filtersätzen**, auf der Sie die verfügbaren Filtersätze organisieren können.
		Wählen Sie ein Filterfeld oder einen Filtersatz aus, nach dem die Ansicht gefiltert werden soll. Wenn Sie auf das Feld klicken, werden alle möglichen Filter und Filtersätze in einem Dropdown-Menü aufgeführt.
	**Filterliste anzeigen**	Wählen Sie die Variablen oder Watchlists aus, nach denen Sie filtern möchten.
	NICHT	Zum Anzeigen von Daten, die mit einigen Filterwerten übereinstimmen und mit anderen nicht, klicken Sie neben die Felder, die Sie ausschließen möchten.
	**ODER**	Zum Anzeigen von Daten, die mit Filtern für reguläre Ausdrücke oder **ODER**-Filtern übereinstimmen, klicken Sie auf dieses Symbol neben den Feldern mit den **ODER**-Werten. Die Ansicht enthält die Daten, die mit den Werten in den nicht mit **ODER** markierten Feldern und mit einem der Werte in den mit **ODER** markierten Feldern übereinstimmen.  Sie müssen mindestens zwei Felder mit **ODER** markieren, damit dieser Filter funktioniert.
	**Groß-/Kleinschreibung ignorieren**	Um die Groß-/Kleinschreibung zu ignorieren, klicken Sie auf dieses Symbol.
	Zeichenfolgennormalisierung	Klicken Sie auf diese Option, um normalisierte Zeichenfolgen durch ihre Aliasse zu ersetzen.
	Filter im Satz anzeigen	Klicken Sie auf diese Option, um eine Liste der in einem Satz enthaltenen Filter anzuzeigen.
	Wert ersetzen	Klicken Sie auf diese Option, um den aktuellen Wert durch den im Wertsatz enthaltenen Wert zu ersetzen.
	**Diesen Filter entfernen**	Klicken Sie auf diese Option, um das Filterfeld aus den aktuellen Filtern zu entfernen.

Hinzufügen von UCF-Filtern und Filtern für Windows-Ereignis-IDs

Eine der Herausforderungen bei der Unterstützung der Compliance in Bezug auf Vorschriften besteht darin, dass sich die Vorschriften ständig ändern. Unified Compliance Framework (UCF) ist ein Unternehmen, das die Details einzelner Vorschriften harmonisierten Kontroll-IDs zuordnet. Bei Änderungen an Vorschriften werden diese IDs aktualisiert und mithilfe von Push an ESM übertragen.

- Sie können nach Compliance-IDs filtern, um die erforderliche Compliance oder bestimmte Unterkomponenten auszuwählen, oder nach Windows-Ereignis-IDs filtern.

Aufgabe	Vorgehensweise
Hinzufügen von UCF-Filtern	1 Klicken Sie im Bereich **Filter** auf das Filtersymbol neben dem Feld **Compliance-ID**. 2 Wählen Sie die Compliance-Werte aus, die Sie als Filter verwenden möchten, und klicken Sie dann auf **OK** | **Abfrage ausführen**  .
Hinzufügen von Filtern für Windows-Ereignis-IDs	1 Klicken Sie auf das Filtersymbol neben der **Signatur-ID**. 2 Wählen Sie in **Filtervariablen** die Registerkarte **Windows** aus. 3 Geben Sie im Textfeld die Windows-Ereignis-IDs (durch Kommas getrennt) ein, oder wählen Sie die Werte, nach denen Sie filtern möchten, in der Liste aus.

Überwachungslisten

Eine *Überwachungsliste* ist eine Gruppierung bestimmter Informationstypen, die Sie als Filter oder Alarmbedingung verwenden können.

Die Watchlist kann global oder spezifisch für einen Benutzer oder eine Gruppe gelten und statisch oder dynamisch sein. Eine *statische Watchlist* besteht aus bestimmten Werten, die Sie eingeben oder importieren. Eine *dynamische Watchlist* besteht aus Werten, die sich aus von Ihnen definierten regulären Ausdrücken oder Suchkriterien für Zeichenfolgen ergeben.

Eine Watchlist kann maximal 1.000.000 Werte enthalten. In der Liste der Werte auf den Seiten **Watchlist hinzufügen** oder **Watchlist bearbeiten** können maximal 25.000 Werte angezeigt werden. Wenn mehr Werte vorhanden sind, werden Sie informiert, dass mehr Werte vorhanden sind als angezeigt werden können. Wenn Sie eine Watchlist bearbeiten möchten, indem Sie Werte hinzufügen, durch die die Gesamtanzahl 25.000 übersteigt, müssen Sie die vorhandene Liste in eine lokale Datei exportieren, die neuen Werte hinzufügen und dann die neue Liste importieren.

Sie können die Werte in einer Watchlist so einrichten, dass sie ablaufen. Der Wert wird mit einem Zeitstempel versehen und läuft ab, wenn die festgelegte Dauer erreicht ist und der Wert nicht aktualisiert wird. Werte werden aktualisiert, wenn ein Alarm ausgelöst wird und die Werte zur Watchlist hinzugefügt werden. Sie können die Werte, für die Ablaufen festgelegt ist, aktualisieren, indem Sie sie mit der Option **An Watchlist anfügen** im Menü einer Ansichtskomponente an die Liste anfügen (siehe *Menüoptionen für Komponenten*).

ESM enthält einen Konnektor für die relationale Datenquelle in Hadoop HBase, von dem die Paare aus Schlüssel und Wert aus der Quelle verwendet werden. Diese Daten können in einer Watchlist verwendet werden (siehe *Hinzufügen einer Hadoop HBase-Watchlist*). Sie können beispielsweise in Alarme einfließen, die ausgelöst werden, wenn in neuen Ereignissen Werte aus der Watchlist gefunden werden.

Hinzufügen einer Überwachungsliste

Fügen Sie eine Überwachungsliste zum ESM-Gerät hinzu, damit Sie sie als Filter oder in einer Alarmbedingung verwenden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Sie haben folgende Möglichkeiten, auf die Seite **Watchlists** zuzugreifen:

- Klicken Sie in der ESM-Konsole auf das Schnellstartsymbol für **Watchlists**  .
- Klicken Sie in der Systemnavigationsstruktur auf die Option **Systemeigenschaften** und dann auf **Watchlists**.

In der Tabelle **Watchlists** werden alle im System vorhandenen Watchlists angezeigt.



Bösartige GTI-IPs und **Verdächtige GTI-IPs** werden in der Tabelle angezeigt, enthalten jedoch nur dann Daten, wenn Sie eine Lizenz für McAfee GTI von McAfee erworben haben. Wenn Sie eine Lizenz erwerben möchten, wenden Sie sich an einen McAfee-Vertriebsingenieur oder an den McAfee-Support.

2 Klicken Sie auf **Hinzufügen**, und geben Sie dann die erforderlichen Informationen ein.

3 Klicken Sie auf OK, um die neue Watchlist zur Tabelle **Watchlists** hinzuzufügen.

Siehe auch

McAfee GTI-Watchlist auf Seite 300

McAfee GTI-Watchlist

McAfee GTI-Watchlists enthalten mehr als 130 Millionen verdächtiger und bösartiger IP-Adressen und deren Schweregrade, die von McAfee gesammelt werden. Mithilfe dieser Watchlists können Sie Alarme auslösen und Daten in Berichten und Ansichten filtern. Sie können als Filter bei der Regelkorrelation und als Bewertungsquelle für einen Risikokorrelations-Manager auf einem ACE-Gerät verwendet werden.

Um die Daten aus den Listen zu Ihrem System hinzuzufügen, müssen Sie eine McAfee GTI-Lizenz von McAfee erwerben. Die Listen werden dann beim nächsten Herunterladen von Regeln zum System hinzugefügt. Aufgrund der Größe der Datenbank kann dieser Vorgang mehrere Stunden dauern.



Zum Herunterladen der Listen benötigen Sie eine Internetverbindung. Die Listen können nicht offline heruntergeladen werden.

Diese Listen können nicht angezeigt oder bearbeitet werden. Aus der Tabelle **Überwachungslisten** (**Systemeigenschaften** | **Überwachungslisten**) geht jedoch hervor, ob die Liste *aktiv* ist (Werte enthält) oder *inaktiv* ist (keine Werte enthält).

Wenn Sie eine McAfee GTI-Lizenz erwerben möchten, wenden Sie sich an einen McAfee-Vertriebsingenieur oder an den McAfee-Support.

Erstellen einer Watchlist für Bedrohungen oder IOC-Feeds aus dem Internet

Sie können eine Watchlist erstellen, die regelmäßig aktualisiert werden kann, um automatisch Feeds für Bedrohungen oder Kompromittierungsindikatoren (Indicators of Compromise, IOC) aus dem Internet abzurufen.

In dieser Watchlist können Sie eine Vorschau der über die HTTP-Anfrage abzurufenden Daten anzeigen und reguläre Ausdrücke zum Filtern dieser Daten hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der Systemnavigationsstruktur auf das System, und klicken Sie dann auf das Symbol **Eigenschaften**  .
2. Klicken Sie auf **Watchlists** und dann auf **Hinzufügen**.
3. Füllen Sie die Registerkarte **Hauptbildschirm** aus, und wählen Sie dabei **Dynamisch** aus.
4. Klicken Sie auf die Registerkarte **Quelle**, und wählen Sie im Feld **Typ** die Option **HTTP/HTTPS** aus.
5. Geben Sie die erforderlichen Informationen auf den Registerkarten **Quelle**, **Analysieren** und **Werte** ein.



Das Feld **Rohdaten** auf der Registerkarte **Analysieren** wird mit den ersten 200 Zeilen des HTML-Quellcodes ausgefüllt. Es handelt sich nur um eine Vorschau der Website, die jedoch ausreicht, um einen regulären Ausdruck für den Vergleich zu schreiben. Wenn Sie **Jetzt ausführen** verwenden oder eine geplante Aktualisierung der Watchlist stattfindet, enthält das Ergebnis alle Übereinstimmungen aus der Suche mit dem regulären Ausdruck. Für diese Funktion werden reguläre Ausdrücke mit RE2-Syntax unterstützt, beispielsweise `(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})` für den Vergleich einer IP-Adresse.

Hinzufügen einer Hadoop HBase-Watchlist

Fügen Sie eine Watchlist mit Hadoop HBase als Quelle hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur das System aus. Klicken Sie auf das Symbol **Eigenschaften**  und dann auf **Watchlists**.
2. Wählen Sie auf der Registerkarte **Hauptbildschirm** des Assistenten **Watchlist hinzufügen** die Option **Dynamisch** aus. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf die Registerkarte **Quelle**.
3. Wählen Sie im Feld **Typen** die Option **Hadoop HBase (REST)** aus. Geben Sie dann den Host-Namen, den Port und den Namen der Tabelle ein.

4 Füllen Sie auf der Registerkarte **Abfrage** die Suchspalte und die Informationen für die Abfrage aus:

a Verwenden Sie in der **Suchspalte** das Format `spaltenFamilie:spaltenName`.

b Füllen Sie die Abfrage mit einem Scanner-Filter aus. Die Werte müssen dabei Base64-codiert sein. Beispiel:

```
<Scanner batch="1024">
<filter>
{
"type": "SingleColumnValueFilter",
"op": "EQUAL",
"family": " ZW1wbG95ZWVJbmZv",
"qualifier": "dXNlcm5hbWU=",
"latestVersion": true,
"comparator": {
"type": "BinaryComparator",
"value": "c2NhcGVnb2F0"
}
}
</filter>
</Scanner>
```

5 Klicken Sie auf die Registerkarte **Werte**, wählen Sie den Werttyp aus, und klicken Sie dann auf die Schaltfläche **Jetzt ausführen**.

Zeichenfolgennormalisierung

Mit der Zeichenfolgennormalisierung können Sie einen Zeichenfolgenwert einrichten, der Alias-Werten zugeordnet werden kann, und eine CSV-Datei mit Zeichenfolgennormalisierungs-Werten importieren oder exportieren.

Dann können Sie die Zeichenfolge und ihre Aliasse filtern, indem Sie neben dem entsprechenden Feld im Bereich **Filter** das Symbol für die Zeichenfolgennormalisierung auswählen. Für die Benutzernamen-Zeichenfolge John Doe definieren Sie eine Zeichenfolgennormalisierungs-Datei. Die primäre Zeichenfolge lautet in diesem Fall `John Doe` und die Aliasse beispielsweise `DoeJohn`, `JDoe`, `john.doe@gmail.com` und `JohnD`. Anschließend können Sie John Doe in das Filterfeld **User_Nickname** eingeben, neben dem Feld das Symbol für den Zeichenfolgennormalisierungs-Filter auswählen und die Abfrage aktualisieren. In der sich ergebenden Ansicht werden alle Ereignisse angezeigt, die John Doe und seinen Aliassen zugeordnet sind. Daher können Sie nach Inkonsistenzen bei der Anmeldung suchen, bei denen zwar die Quell-IPs, aber nicht die Benutzernamen übereinstimmen. Diese Funktion ist auch hilfreich, wenn Sie Vorschriften einhalten müssen, die das Melden von Aktivitäten berechtigter Benutzer vorsehen.

Verwalten von Zeichenfolgennormalisierungs-Dateien

Damit Sie eine Zeichenfolgennormalisierungs-Datei verwenden können, müssen Sie sie zum ESM-Gerät hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Bereich **Filter** auf das Symbol **Manager für die Normalisierung von Zeichenfolgen starten**  .

2 Führen Sie eine oder mehrere der verfügbaren Aktionen aus, und klicken Sie dann auf **Schließen**.

Erstellen einer Zeichenfolgennormalisierungs-Datei zum Importieren

Wenn Sie eine CSV-Datei mit Aliassen erstellen, können Sie diese auf der Seite **Zeichenfolgennormalisierung** importieren, sodass sie als Filter verwendet werden kann.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Geben Sie in einem Textverarbeitungs- oder Tabellenkalkulationsprogramm die Aliasse im folgenden Format ein:

```
Befehl, primäre Zeichenfolge, Alias
```

Die möglichen Befehle lauten `Hinzufügen`, `Ändern` und `Löschen`.

2 Speichern Sie die Datei als CSV-Datei, und importieren Sie diese.

Benutzerdefinierte Typfilter

Sie können benutzerdefinierte Typfelder als Filter für Ansichten und Berichte verwenden, um die für Sie relevantesten Daten zu definieren und auf diese zuzugreifen.

Die von diesen benutzerdefinierten Typfeldern generierten Daten können Sie in der Ansicht **Ereignisanalyse** oder **Flussanalyse** im Abschnitt **Details** anzeigen.

Sie können benutzerdefinierte Typen hinzufügen, bearbeiten oder entfernen sowie exportieren und importieren. Auf der Seite **Bearbeiten** können Sie den Namen ändern. Bei einem benutzerdefinierten Datentyp können Sie außerdem die Einstellungen für Untertypen ändern.

Exportieren oder Importieren benutzerdefinierter Typen

Wenn Sie benutzerdefinierte Typen exportieren, werden alle an den ausgewählten Speicherort exportiert. Wenn Sie eine Datei mit benutzerdefinierten Typen importieren, werden die aktuellen benutzerdefinierten Typen im System durch die importierten Daten ersetzt.

Benutzerdefinierte Abfragen

Wenn Sie eine benutzerdefinierte Abfrage für eine Ansicht einrichten, werden die vordefinierten benutzerdefinierten Typen bei der Auswahl der Felder für die Abfrage als Optionen angezeigt. Wenn Sie einen benutzerdefinierten Typ als Feld in der Abfrage hinzufügen, fungiert dieser als Filter. Wenn die abgefragten Informationen keine Daten für diesen benutzerdefinierten Typ enthalten, wird die Abfragetabelle ohne Ergebnisse zurückgegeben. Dies können Sie verhindern, indem Sie das Benutzerfeld (Benutzerdefiniertes Feld 1 bis 10 in der Tabellenspalte **Ereignisfeld**) auswählen, sodass anstelle des benutzerdefinierten Typs die benötigten Ergebnisse zurückgegeben werden.

Beispiel: Die Abfrageergebnisse sollen Quellbenutzerdaten enthalten, sofern diese vorhanden sind. Wenn Sie **Quellbenutzer** als Abfragefeld auswählen, fungiert das Feld als Filter, und wenn die abgefragten Informationen keine Quellbenutzerdaten enthalten, werden von der Abfrage keine Ergebnisse zurückgegeben. Wenn Sie jedoch das Benutzerfeld 7 auswählen, das als Benutzerfeld für Quellbenutzer vorgesehen ist, fungiert das Feld nicht als Filter und wird in der Ergebnistabelle als Spalte angezeigt. Vorhandene Quellbenutzerdaten werden in dieser Spalte angezeigt. Wenn für das Feld keine Daten vorhanden sind, ist die Spalte Benutzerfeld 7 leer, während die anderen Spalten ausgefüllt sind.

Benutzerdefinierter Datentyp

Wenn Sie im Feld **Datentyp** die Option **Benutzerdefiniert** auswählen, können Sie die Bedeutung der einzelnen Felder in einem Protokoll mit mehreren Feldern definieren.

Ein Protokoll (100300.351) enthält beispielsweise drei Felder (100, 300,35, 1). Mit dem benutzerdefinierten Untertyp können Sie festlegen, worum es sich bei den einzelnen Feldern handelt (Ganzzahl, Dezimalzahl, boolescher Wert). Beispiel:

- Anfängliches Protokoll: `100300.351`
- Drei Untertypen: `Ganzzahl|Dezimalformat|Boolescher Wert`
- Benutzerdefinierter Untertyp: `100|300,35|1`



Die Untertypen können maximal 8 Bytes (64 Bits) an Daten enthalten. In **Speicherplatzverwendung**: wird die Anzahl der verwendeten Bytes und Bits angezeigt. Wenn das Maximum überschritten ist, wird in diesem Feld in Rot darauf hingewiesen, dass der Speicherplatz überschritten ist. Beispiel:
`Speicherplatzverwendung: 9 von 8 Bytes, 72 von 64 Bits.`

Name/Wert, benutzerdefinierter Typ

Wenn Sie den Datentyp **Name/Wert-Gruppe** auswählen, können Sie einen benutzerdefinierten Typ hinzufügen, der eine Gruppe von Name/Wert-Paaren enthält, die Sie angeben. Dann können Sie Ansichten und Abfragen nach diesen Paaren filtern und sie in Feldübereinstimmungsalarmen verwenden.

Diese Funktion hat unter anderem die folgenden Merkmale:

- Die Felder für Name/Wert-Gruppen müssen mit einem regulären Ausdruck gefiltert werden.
- Die Paare können korreliert werden, sodass sie im **Editor für Korrelationsregeln** ausgewählt werden können.
- Die Werte in dem Paar können nur über den erweiterten Syslog-Parser (Advanced Syslog Parser, ASP) erfasst werden.
- Für diesen benutzerdefinierten Typ gilt eine maximale Größe von 512 Zeichen einschließlich der Namen. Längere Werte werden bei der Erfassung abgeschnitten. McAfee empfiehlt, die Größe und Anzahl der Namen zu begrenzen.
- Die Namen müssen aus mehr als zwei Zeichen bestehen.
- Der benutzerdefinierte Typ für Name/Wert kann bis zu 50 Namen enthalten.
- Jeder Name in der Name/Wert-Gruppe wird im globalen Filter in der Schreibweise <Name der Gruppe> - <Name> angezeigt.

Format für reguläre Ausdrücke für nicht indizierte benutzerdefinierte Typen

Verwenden Sie dieses Format für nicht indizierte und indizierte benutzerdefinierte Typen für Zeichenfolgen, zufällige Zeichenfolgen und Zeichenfolgen-Hashs:

- Sie können die Syntax `contains(<regulärer Ausdruck>)` verwenden oder einfach einen Wert in die Felder für nicht indizierte zufällige Zeichenfolgen oder Zeichenfolgen-Hashs eingeben und dann benutzerdefinierte Typen filtern.
- Sie können die Syntax `regex()` verwenden.
- Wenn Sie `contains()` verwenden und einen durch Komma getrennten Filter in einem Feld für nicht indizierte benutzerdefinierte Typen verwenden (Tom,John,Steve), wird vom System ein regulärer Ausdruck ausgeführt. Das Komma und das Sternchen fungieren als Pipe (|) und als Punkt gefolgt von einem Sternchen (.*) in einem contains-Feld, einem Feld für nicht indizierte zufällige Zeichenfolgen oder einem Feld für Zeichenfolgen-Hashs. Wenn Sie ein Zeichen wie beispielsweise ein Sternchen (*) eingeben, wird es durch einen Punkt gefolgt von dem Sternchen ersetzt (.*).
- Ein ungültiger regulärer Ausdruck. oder eine fehlende schließende Klammer können zu einem Fehler führen, bei dem Sie informiert werden, dass der reguläre Ausdruck ungültig ist.

- Sie können nur einen einzelnen `regex()` oder `contains()`-Wert in Feldern für benutzerdefinierte Typen mit nicht indizierten oder indizierten Zeichenfolgen, zufälligen Zeichenfolgen und Zeichenfolgen-Hashs verwenden.
- Im Feld Signatur-ID können Sie jetzt `contains(<Teil einer Regelnachricht oder gesamte Regelnachricht>)` und `regex(<Teil einer Regelnachricht>)` verwenden.
- Ein allgemeiner Suchfilter für `contains` ist ein einzelner Wert, nicht ein einzelner Wert mit einem `.*` davor und dahinter.

Beispiele für allgemeine Suchfilter:

- Ein einzelner Wert
- Mehrere durch Kommas getrennte Werte, die in einen regulären Ausdruck konvertiert werden.
- Eine `contains` Anweisung mit einem *, das als .* fungiert.
- Erweiterte reguläre Ausdrücke, für die Sie die Syntax `regex()` verwenden können.

Weitere Informationen finden Sie unter *Beschreibung der `contains`-Filter und Filter für `reguläre Ausdrücke`* .

Erstellen benutzerdefinierter Typen

Wenn Sie über Administratorberechtigungen verfügen, können Sie benutzerdefinierte Typen hinzufügen, um sie als Filter zu verwenden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur die Option **Systemeigenschaften** aus, und klicken Sie dann auf **Benutzerdefinierte Typen**.
2. Klicken Sie auf **Hinzufügen**, und geben Sie dann die erforderlichen Informationen ein.
3. Klicken Sie auf **OK**, um den benutzerdefinierten Typ zu speichern.

Tabelle der vordefinierten benutzerdefinierten Typen

Wenn Sie über Administratorberechtigungen verfügen, können Sie eine Liste der vordefinierten benutzerdefinierten Typen in der Tabelle der benutzerdefinierten Typen anzeigen (**Systemeigenschaften** | **Benutzerdefinierte Typen**). Wenn Sie nicht über Administratorberechtigungen verfügen, verwenden Sie diese Liste der vordefinierten benutzerdefinierten Typen.

Name	Datentyp	Ereignisfeld	Flussfeld
Application	Zeichenfolge	Benutzerdefiniertes Feld 1	Keines
Application_Layer	Signatur-ID	Keines	Benutzerdefiniertes Feld 4
Application_Protocol	Zeichenfolge	Benutzerdefiniertes Feld 1	Keines
Authoritative_Answer	Zeichenfolge	Benutzerdefiniertes Feld 10	Keines
Bcc	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
Cc	Zeichenfolge	Benutzerdefiniertes Feld 8	Keines

Name	Datentyp	Ereignisfeld	Flussfeld
Client_Version	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
Befehl	Zeichenfolge	Benutzerdefiniertes Feld 2	Keines
Confidence (verlässigkeit)	Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 8	Keines
Contact_Name	Zeichenfolge	Benutzerdefiniertes Feld 6	Keines
Contact_Nickname	Zeichenfolge	Benutzerdefiniertes Feld 8	Keines
Cookie	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
Database_Name	Zeichenfolge	Benutzerdefiniertes Feld 8	Keines
Destination User (Zielbenutzer)	Zeichenfolge	Benutzerdefiniertes Feld 6	Benutzerdefiniertes Feld 1
Destination_Filename	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
Richtung	Zeichenfolge	Benutzerdefiniertes Feld 10	Keines
DNS_Class	Zeichenfolge	Benutzerdefiniertes Feld 8	Keines
DNS_Name	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
DNS_Type	Zeichenfolge	Benutzerdefiniertes Feld 6	Keines
Domäne	Zeichenfolge	Benutzerdefiniertes Feld 3	Keines
End_Page	Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 9	Keines
File_Operation	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
File_Operation_Succeeded	Zeichenfolge	Benutzerdefiniertes Feld 6	Keines
Dateiname	Zeichenfolge	Benutzerdefiniertes Feld 3	Keines
Flow_Flags	Nicht signierte Ganzzahl	Keines	Benutzerdefiniertes Feld 1
Von	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
Hops	Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 8	Keines
Host	Zeichenfolge	Benutzerdefiniertes Feld 4	Keines
HTTP_Layer	Signatur-ID	Keines	Benutzerdefiniertes Feld 5
HTTP_Req_Cookie	Zeichenfolge	Keines	Benutzerdefiniertes Feld 3

Name	Datentyp	Ereignisfeld	Flussfeld
HTTP_Req_Host	Zeichenfolge	Keines	Benutzerdefiniertes Feld 5
HTTP_Req_Method	Zeichenfolge	Keines	Benutzerdefiniertes Feld 6
HTTP_Req_Reference	Zeichenfolge	Keines	Benutzerdefiniertes Feld 4
HTTP_Req_URL	Zeichenfolge	Keines	Benutzerdefiniertes Feld 2
HTTP_Resp_Length	Nicht signierte Ganzzahl	Keines	Benutzerdefiniertes Feld 5
HTTP_Resp_Status	Nicht signierte Ganzzahl	Keines	Benutzerdefiniertes Feld 4
HTTP_Resp_TTFB	Nicht signierte Ganzzahl	Keines	Benutzerdefiniertes Feld 6
HTTP_Resp_TTLB	Nicht signierte Ganzzahl	Keines	Benutzerdefiniertes Feld 7
HTTP_User_Agent	Zeichenfolge	Keines	Benutzerdefiniertes Feld 7
Schnittstelle	Zeichenfolge	Benutzerdefiniertes Feld 8	Keines
Job_Name	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
Sprache	Zeichenfolge	Benutzerdefiniertes Feld 10	Keines
Local_User_Name	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
Message_Text	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
Methode	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
Nat_Details • NAT_Address • NAT_Port • NAT_Type	Benutzerdefiniert • IPv4-Adresse • Nicht signierte Ganzzahl • Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 9	Benutzerdefiniertes Feld 1
Network_Layer	Signatur-ID	Keines	Benutzerdefiniertes Feld 1
NTP_Client_Mode	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
NTP_Offset_To_Monitor	Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 8	Keines
NTP_Opcode	Zeichenfolge	Benutzerdefiniertes Feld 10	Keines
NTP_Request	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
NTP_Server_Mode	Zeichenfolge	Benutzerdefiniertes Feld 6	Keines

Name	Datentyp	Ereignisfeld	Flussfeld
Num_Copies	Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 6	Keines
Objekt	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
Object_Type	Zeichenfolge	Benutzerdefiniertes Feld 2	Keines
Priorität	Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 8	Keines
Query_Response	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
Referenz	Zeichenfolge	Benutzerdefiniertes Feld 10	Keines
Antwortzeit • Sekunden • Millisekunden	Benutzerdefiniert • Nicht signierte Ganzzahl • Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 10	Keines
RTMP_Application	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
Session_Layer	Zeichenfolge	Keines	Benutzerdefiniertes Feld 3
SNMP_Error_Code	Zeichenfolge	Benutzerdefiniertes Feld 10	Keines
SNMP_Item	Zeichenfolge	Benutzerdefiniertes Feld 6	Keines
SNMP_Item_Type	Zeichenfolge	Benutzerdefiniertes Feld 8	Keines
SNMP_Operation	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
SNMP_Version	Zeichenfolge	Benutzerdefiniertes Feld 9	Keines
Source User (Quellbenutzer)	Zeichenfolge	Benutzerdefiniertes Feld 7	
Start_Page	Nicht signierte Ganzzahl	Benutzerdefiniertes Feld 8	Keines
Betreff	Zeichenfolge	Benutzerdefiniertes Feld 10	Keines
SWF_URL	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
TC_URL	Zeichenfolge	Benutzerdefiniertes Feld 6	Keines
An	Zeichenfolge	Benutzerdefiniertes Feld 6	Keines
Transport_Layer	Signatur-ID	Keines	Benutzerdefiniertes Feld 2
URL	Zeichenfolge	Benutzerdefiniertes Feld 8	Keines

Name	Datentyp	Ereignisfeld	Flussfeld
User_Agent	Zeichenfolge	Benutzerdefiniertes Feld 6	Keines
User_Nickname	Zeichenfolge	Benutzerdefiniertes Feld 5	Keines
Version	Zeichenfolge	Benutzerdefiniertes Feld 10	Keines

Hinzufügen benutzerdefinierter Typen für die Uhrzeit

Sie können benutzerdefinierte Typen hinzufügen, mit denen Sie Uhrzeitdaten speichern können.

Uhrzeit: Genauigkeit für Sekunden speichert Uhrzeitdaten auf die Sekunde genau. **Uhrzeit: Genauigkeit für Nanosekunden** speichert die Uhrzeit auf die Nanosekunde genau. Dazu gehört eine Gleitkommazahl mit neun Genauigkeitswerten, die die Nanosekunden darstellen.

Wenn Sie beim Hinzufügen dieses benutzerdefinierten Typs die Option **Index** auswählen, wird das Feld in Abfragen, Ansichten und Filtern als Filter angezeigt. Es wird nicht in Verteilungskomponenten angezeigt und ist in Datenanreicherungen, Watchlists oder Alarmen nicht verfügbar.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System aus. Klicken Sie auf das Symbol **Eigenschaften** und dann auf **Benutzerdefinierte Typen** | **Hinzufügen**.

2 Klicken Sie im Feld **Datentyp** auf **Uhrzeit: Genauigkeit für Sekunden** oder **Uhrzeit: Genauigkeit für Nanosekunden**, geben Sie die verbleibenden Informationen ein, und klicken Sie dann auf **OK**.

Benutzerdefinierte Typen für Name/Wert

Der benutzerdefinierte Typ für Name/Wert besteht aus einer Gruppe von Name/Wert-Paaren, die Sie angeben. Sie können Ansichten und Abfragen nach diesen Paaren filtern und sie in Alarmen vom Typ **Interne Ereignisübereinstimmung** verwenden.

Diese Funktion hat unter anderem die folgenden Merkmale:

- Die Felder für Name/Wert-Gruppen müssen mit einem regulären Ausdruck gefiltert werden.
- Sie können korreliert werden, sodass sie im **Editor für Korrelationsregeln** ausgewählt werden können.
- Die Werte in dem Paar können nur über ASP erfasst werden.
- Für diesen benutzerdefinierten Typ gilt eine maximale Größe von 512 Zeichen einschließlich der Namen. Zeichen nach dem 512. Zeichen werden bei der Erfassung abgeschnitten. McAfee empfiehlt, die Größe und Anzahl der Namen zu begrenzen.
- Die Namen müssen aus mehr als zwei Zeichen bestehen.
- Der benutzerdefinierte Typ für Name/Wert kann bis zu 50 Namen enthalten.
- Jeder Name in der Name/Wert-Gruppe wird im globalen Filter in der Schreibweise <Name der Gruppe> - <Name> angezeigt.

Hinzufügen eines benutzerdefinierten Typs für eine Name/Wert-Gruppe

Wenn Sie eine Gruppe von Name/Wert-Paaren hinzufügen, können Sie Ansichten und Abfragen nach diesen Paaren filtern und sie in Alarmen vom Typ **Interne Ereignisübereinstimmung** verwenden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie in der Systemnavigationsstruktur das System aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

2 Klicken Sie auf **Benutzerdefinierte Typen** und dann auf **Hinzufügen**.

3 Klicken Sie im Feld **Datentyp** auf **Name/Wert-Gruppe**, geben Sie die verbleibenden Informationen ein, und klicken Sie dann auf **OK**.

8 Verwalten von Fällen

Mit der Fallverwaltung von ESM können Sie Arbeitselemente und Support-Tickets, die Netzwerkereignissen zugeordnet sind, zuweisen und verfolgen. Damit Sie auf diese Funktion zugreifen können, müssen Sie einer Gruppe angehören, für die die Berechtigung **Fallverwaltungsbenutzer** aktiviert ist.

Sie haben fünf Möglichkeiten, einen Fall hinzuzufügen:

- In der Ansicht **Fallverwaltung**
- Im Bereich **Fälle** ohne Verknüpfung mit einem Ereignis
- In der Ansicht **Ereignisanalyse** mit Verknüpfung mit einem Ereignis
- Beim Einrichten eines Alarms
- In einer Benachrichtigung über einen ausgelösten Alarm

Inhalt

- *Hinzufügen eines Falls*
- *Erstellen eines Falls aus einem Ereignis*
- *Hinzufügen von Ereignissen zu einem vorhandenen Fall*
- *Bearbeiten oder Schließen eines Falls*
- *Anzeigen von Falldetails*
- *Hinzufügen von Fallstatusebenen*
- *Senden von Fällen per E-Mail*
- *Anzeigen aller Fälle*
- *Generieren von Fallverwaltungsberichten*

Hinzufügen eines Falls

Beim Verfolgen eines Tasks, der als Ergebnis eines Netzwerkereignisses generiert wurde, fügen Sie als Erstes im Fallverwaltungssystem einen Fall hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Bereich **Fälle** auf das Symbol **Fall hinzufügen**  .

2 Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Der Fall wird zu dem Bereich **Fälle** des Benutzers hinzugefügt, dem der Fall zugewiesen wird. Wenn Sie **Fall per E-Mail senden** ausgewählt haben, wird außerdem eine E-Mail gesendet (siehe *Senden eines Falls per E-Mail*).

Erstellen eines Falls aus einem Ereignis

Zum Verfolgen eines Ereignisses in der Ansicht **Ereignisanalyse** erstellen Sie einen Fall. Damit wird die Workflow-Überwachung aktiviert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Liste der Ansichten die folgenden Optionen aus: **Ereignisansichten** | **Ereignisanalyse**.
2. Klicken Sie auf das Ereignis, klicken Sie auf das Menüsymbol  und dann auf **Aktionen** | **Neuen Fall erstellen**.
3. Geben Sie die erforderlichen Informationen ein, und klicken Sie anschließend auf **OK**, um den Fall zu speichern.

Der neue Fall enthält die Ereignisdaten in der Tabelle **Nachricht**.

Hinzufügen von Ereignissen zu einem vorhandenen Fall

Sie können zu einem vorhandenen Fall mindestens ein Ereignis hinzufügen, um Aktionen nachzuverfolgen, die als Reaktion auf diese Ereignisse ausgeführt wurden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie im Ansichtsbereich in der Dropdown-Liste mit den Ansichten die Option **Ereignisansichten** aus, und klicken Sie dann auf **Ereignisanalyse**.
2. Wählen Sie die Ereignisse aus, und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie auf das Symbol **Ereignisse zu einem Fall oder zu Remedy zuweisen**  , und wählen Sie **Ereignisse zu einem Fall hinzufügen** aus.
   - Klicken Sie auf das Symbol **Menü**  , heben Sie **Aktionen** hervor, und klicken Sie dann auf **Ereignisse zu einem Fall hinzufügen**.
3. Wählen Sie den Fall aus, und klicken Sie auf **Hinzufügen**.

   Auf der Seite **Falldetails** wird in der Tabelle **Nachrichten** die Ereignis-ID angezeigt.
4. Klicken Sie auf **OK** und dann auf **Schließen**.

Bearbeiten oder Schließen eines Falls

Wenn Sie über Berechtigungen als **Fallverwaltungsadministrator** verfügen, können Sie alle Fälle im System ändern. Wenn Sie über Berechtigungen als **Fallverwaltungsbenutzer** verfügen, können Sie nur Fälle ändern, die Ihnen zugewiesen sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Greifen Sie mit einer der folgenden Methoden auf **Falldetails** zu.

Art des Falls	Vorgehensweise
Ein Ihnen zugewiesener Fall	1 Wählen Sie den Fall im Bereich **Fälle** aus. 2 Klicken Sie auf das Symbol **Fall bearbeiten** .
Ein nicht Ihnen zugewiesener Fall	1 Klicken Sie auf das Symbol **Fallverwaltung öffnen** im Bereich **Fälle**. 2 Wählen Sie den Fall aus, den Sie ändern möchten. 3 Klicken Sie unten in der Ansicht auf das Symbol **Fall bearbeiten** .

2 Bearbeiten Sie die Einstellungen, oder schließen Sie den Fall im Feld **Status**.

3 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Die Änderungen werden auf der Seite **Falldetails** im Abschnitt **Hinweise** aufgezeichnet. Wenn Sie den Fall geschlossen haben, wird er im Bereich **Fälle** nicht mehr angezeigt. In der Liste **Fallverwaltung** bleibt er jedoch sichtbar, und der Status lautet jetzt **Abgeschlossen**.

Anzeigen von Falldetails

Wenn Sie über **Administratorrechte** auf dem ESM-Gerät verfügen, können Sie alle Fälle auf dem ESM-Gerät anzeigen und Aktionen für sie ausführen. Alle Benutzer in einer Gruppe können alle Fälle in dieser Gruppe anzeigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Bereich **Fälle** auf das Symbol **Fallverwaltung öffnen** .

Die Ansicht **Fallverwaltung** wird geöffnet. Sie enthält eine Liste aller Fälle im System.

2 Überprüfen Sie die Daten auf den Registerkarten **Hinweise** und **Quellereignisse**.

3 Doppelklicken Sie auf einen Fall, um weitere Details anzuzeigen, und überprüfen Sie dann die Informationen auf der Seite **Falldetails**.

Hinzufügen von Fallstatusebenen

Der Fall-Manager enthält zwei Statusebenen: **Offen** und **Abgeschlossen**. Sie können weitere Status hinzufügen, denen Fälle zugewiesen werden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Bereich **Fälle** auf das Symbol **Fallverwaltung öffnen** .

2 Klicken Sie in der Ansicht **Fallverwaltung** auf der unteren Symbolleiste auf das Symbol **Fallverwaltungseinstellungen** und dann auf **Hinzufügen**.

3 Geben Sie einen Namen für den Status ein, und wählen Sie dann aus, ob der Status als Standard für neue Fälle verwendet werden soll.

4 Wählen Sie aus, ob Fälle mit diesem Status im Bereich **Fälle** angezeigt werden sollen, und klicken Sie dann auf **OK**.

Senden von Fällen per E-Mail

Richten Sie das System so ein, dass beim Hinzufügen oder erneuten Zuweisen eines Falls immer automatisch eine E-Mail an die Person oder Gruppe gesendet wird, der der Fall zugewiesen ist.

Bevor Sie beginnen

Sie müssen über Berechtigungen als **Fallverwaltungsadministrator** verfügen.

Außerdem können Sie manuell eine Fallbenachrichtigung per E-Mail senden und dabei Fallhinweise und Ereignisdetails einschließen.

Aufgabe	Vorgehensweise
Automatisches Senden eines Falls per E-Mail	1 Klicken Sie im Bereich **Fälle** auf das Symbol **Fenster Fallverwaltung öffnen**. 2 Klicken Sie auf das Symbol **Fallverwaltungseinstellungen**. 3 Wählen Sie **Beim Zuweisen eines Falls eine E-Mail senden** aus, und klicken Sie dann auf **Schließen**. Die E-Mail-Adressen der Benutzer müssen auf dem ESM-Gerät vorhanden sein (siehe *Einrichten von Benutzergruppen*).
Manuelles Senden eines vorhandenen Falls per E-Mail	1 Wählen Sie auf der Seite **Fälle** den Fall aus, den Sie per E-Mail senden möchten. Klicken Sie dann auf das Symbol **Fall bearbeiten**. 2 Klicken Sie in **Falldetails** auf **Fall per E-Mail senden**, und füllen Sie dann die Felder **Von** und **An** aus. 3 Wählen Sie aus, ob Sie die Hinweise einschließen und eine CSV-Datei mit den Ereignisdetails anfügen möchten. 4 Geben Sie Hinweise ein, die Sie in die E-Mail-Nachricht einschließen möchten, und klicken Sie dann auf **Senden**.

Anzeigen aller Fälle

Wenn Sie über **Administrative** Berechtigungen auf dem ESM-Gerät verfügen, können Sie alle zurzeit geöffneten oder abgeschlossenen Fälle im System verwalten. Mit **Fallverwaltungsadministrator**-Berechtigungen können Sie Status und Unternehmen erstellen sowie die Funktion für automatische E-Mails festlegen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im Bereich **Fälle** auf das Symbol **Fallverwaltung öffnen**.

Die Ansicht **Fallverwaltung** wird geöffnet.

2 Führen Sie einen oder mehrere der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Hinzufügen eines Falls	Klicken Sie auf der Symbolleiste unten in der Ansicht auf das Symbol **Fall hinzufügen**  .
Anzeigen oder Bearbeiten des ausgewählten Falls	Klicken Sie auf der Symbolleiste unten in der Ansicht auf das Symbol **Fall bearbeiten**  .
Senden des ausgewählten Falls per E-Mail	Klicken Sie auf der Symbolleiste unten in der Ansicht auf das Symbol **Fall per E-Mail senden**  .
Einrichten eines Falls, für den beim Hinzufügen oder Ändern eine E-Mail gesendet wird	Klicken Sie auf der Symbolleiste unten in der Ansicht auf das Symbol **Fallverwaltungseinstellungen**  .
Hinzufügen oder Bearbeiten der für Fälle verfügbaren Status	Klicken Sie auf das Symbol **Fallverwaltungseinstellungen**  und dann auf **Hinzufügen**, **Bearbeiten** oder **Löschen**.
Anzeigen der Hinweise, des Verlaufs und der Quellereignisse für den ausgewählten Fall	Klicken Sie auf **Hinweise**, **Verlauf** oder **Quellereignisse**. Wenn Sie auf **Quellereignisse** klicken, werden die Registerkarten für **Quellereignisdetails** geöffnet. Wenn die Registerkarten nicht angezeigt werden oder Sie die angezeigten Registerkarten ausblenden möchten, klicken Sie auf der Symbolleiste unten in der Ansicht auf das Symbol **Quellereignisdetails anzeigen**  . Auf der Registerkarte **Verlauf** wird aufgezeichnet, wann Benutzer einen Fall anzeigen. Wenn ein Benutzer einen Fall innerhalb von fünf Minuten mehrmals anzeigt, wird der Datensatz nicht jedes Mal aktualisiert.
Filtern der Fälle	Wählen Sie im Bereich **Filter** die Daten zum Filtern der Fälle aus, oder geben Sie sie ein. Klicken Sie dann auf das Symbol **Abfrage ausführen**  . Die Liste der Fälle wird geändert, sodass nur die den Filterkriterien entsprechenden Fälle angezeigt werden.

Generieren von Fallverwaltungsberichten

Auf dem ESM-Gerät stehen drei Fallverwaltungsberichte zur Verfügung.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf der Seite **Systemeigenschaften** auf **Berichte** | **Hinzufügen**.

2 Füllen Sie die Abschnitte 1, 2 und 3 aus.

3 Wählen Sie in Abschnitt 4 die Option **CSV-Datei für Abfrage** aus.

4 Wählen Sie in Abschnitt 5 den Fallverwaltungsbericht aus, den Sie ausführen möchten.

- **Zusammenfassung für die Fallverwaltung**: Enthält die Fall-IDs, die den Fällen zugewiesenen Schweregrade, ihren Status, die Benutzer, denen die Fälle zugewiesen sind, gegebenenfalls die Unternehmen, in denen sie zugewiesen sind, Datum und Uhrzeit des Zeitpunkts, zu dem die Fälle hinzugefügt wurden, gegebenenfalls Datum und Uhrzeit des Zeitpunkts, zu dem die Fälle aktualisiert wurden, und die Fallzusammenfassungen.
- **Details für die Fallverwaltung**: Enthält alle Informationen des Berichts **Zusammenfassung für die Fallverwaltung** sowie die IDs der mit den Fällen verknüpften Ereignisse und die im Hinweisabschnitt der Fälle enthaltenen Informationen.
- **Zeitbedarf für die Auflösung des Falls**: Zeigt an, wie viel Zeit zwischen Statusänderungen verstrichen ist (beispielsweise den Abstand zwischen den Zeitstempeln für **Offen** und **Abgeschlossen**). Standardmäßig werden die Fälle mit dem Status **Abgeschlossen** nach **Fall-ID** sowie nach Schweregrad, Unternehmen, Zeitpunkt für **Erstellt**, letzte Aktualisierung, Zusammenfassung und Zeitunterschied aufgeführt.
- **Fälle nach Beauftragtem**: Enthält die Anzahl der Fälle, die einem Benutzer oder einer Gruppe zugewiesen sind.
- **Fälle nach Unternehmen**: Enthält die Anzahl der Fälle nach Unternehmen.
- **Fälle nach Status**: Enthält die Anzahl der Fälle nach Statustyp.

5 Füllen Sie Abschnitt 6 aus (siehe *Beschreibung der* `contains`*-Filter und Filter für* `reguläre Ausdrücke`), und klicken Sie dann auf **Speichern**.

Der Bericht wird gespeichert und zur Liste **Berichte** hinzugefügt.

9 Arbeiten mit Asset Manager

Mit **Asset Manager** können Sie Ressourcen zentral entdecken, manuell erstellen und importieren.

Auf der Registerkarte **Ressource** können Sie eine Gruppe erstellen, die eine oder mehrere Ressourcen enthalten soll. Sie können die folgenden Vorgänge für die gesamte Gruppe ausführen:

- Ändern der Attribute für alle Ressourcen in der Gruppe

  Diese Änderung ist nicht dauerhaft. Wenn Sie eine Ressource zu einer geänderten Gruppe hinzufügen, erbt die Ressource nicht automatisch die vorherigen Einstellungen.

- Verschieben über Drag-and-drop
- Umbenennen einer Gruppe bei Bedarf

Mithilfe von Ressourcengruppen haben Sie mehr Möglichkeiten zum Kategorisieren von Ressourcen als mit der Kennzeichnung von Ressourcen. Beispiel: Sie möchten für jedes Gebäude auf Ihrem Firmengelände eine Ressourcengruppe erstellen. Die Ressource besteht aus einer IP-Adresse und einer Sammlung von Tags. Mit den Tags beschreiben Sie das auf der Ressource ausgeführte Betriebssystem und eine Sammlung der Dienste, für die die Ressource zuständig ist.

Es gibt zwei Möglichkeiten, die Tags einer Ressource zu definieren: Durch das System, wenn eine Ressource abgerufen wird, oder durch den Benutzer, wenn eine Ressource hinzugefügt oder bearbeitet wird. Vom System eingerichtete Tags werden bei jedem Abruf der Ressource aktualisiert, wenn sie geändert wurden. Vom Benutzer eingerichtete Tags werden beim Abruf der Ressource nicht aktualisiert, auch dann nicht, wenn sie geändert wurden. Wenn Sie die Tags einer Ressource hinzufügen oder bearbeiten, die Tags jedoch beim Abruf der Ressource vom System aktualisiert werden sollen, klicken Sie auf **Zurücksetzen**. Diese Aktion müssen Sie jedes Mal ausführen, wenn Sie die Tag-Einstellungen ändern.

Die Konfigurationsverwaltung ist Bestandteil von standardmäßigen Compliance-Vorschriften wie beispielsweise PCI, HIPPA und SOX. Mit dieser Funktion können Sie alle Änderungen überwachen, die möglicherweise an der Konfiguration von Routern und Switches vorgenommen werden, und damit Systemschwachstellen verhindern. Auf dem ESM-Gerät können Sie mit der Funktion für die Konfigurationsverwaltung folgende Aufgaben ausführen:

- Festlegen der Abfragehäufigkeit für Geräte
- Auswählen der entdeckten Geräte, deren Konfiguration überprüft werden soll
- Identifizieren einer abgerufenen Konfigurationsdatei als Standard für das Gerät
- Anzeigen der Konfigurationsdaten, Herunterladen der Daten in eine Datei und Vergleichen der Konfigurationsinformationen der beiden Geräte

Inhalt

- *Verwalten von Ressourcen*
- *Einrichten der Konfigurationsverwaltung*
- *Netzwerkerkennung*
- *Ressourcenquellen*

- *Verwalten von Vulnerability Assessment-Quellen*
- *Zonenverwaltung*
- *Bewertung von Ressourcen, Bedrohungen und Risiken*
- *Verwalten bekannter Bedrohungen*

Verwalten von Ressourcen

Eine Ressource ist ein beliebiges Gerät im Netzwerk, das über eine IP-Adresse verfügt.

Auf der Registerkarte **Ressource** in **Asset Manager** können Sie Ressourcen erstellen, ihre Tags ändern, Ressourcengruppen erstellen, Ressourcenquellen hinzufügen und eine Ressource zu einer Ressourcengruppe hinzufügen. Außerdem können Sie die Ressourcen ändern, die von einem der Vulnerability Assessment-Anbieter erlernt wurden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf das Schnellstartsymbol für **Asset Manager**  .

2 Vergewissern Sie sich, dass die Registerkarte **Ressource** ausgewählt ist.

3 Verwalten Sie die Ressourcen nach Bedarf, und klicken Sie dann auf **OK**.

Aufgaben

- *Definieren alter Ressourcen* auf Seite 318
  In der Gruppe **Alte Ressourcen** in **Asset Manager** können Sie Ressourcen speichern, die im definierten Zeitraum nicht entdeckt wurden.

Definieren alter Ressourcen

In der Gruppe **Alte Ressourcen** in **Asset Manager** können Sie Ressourcen speichern, die im definierten Zeitraum nicht entdeckt wurden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf das Schnellstartsymbol für **Asset Manager**  .

2 Doppelklicken Sie auf der Registerkarte **Ressource** in der Liste der Ressourcen auf die Gruppe **Alte Ressourcen**.

3 Wählen Sie aus, wie viele Tage seit der letzten Entdeckung einer Ressource vergangen sein müssen, damit sie in den Ordner **Alte Ressourcen** verschoben werden muss. Klicken Sie dann auf **OK**.

Einrichten der Konfigurationsverwaltung

Bei der Konfigurationsverwaltung werden die Konfigurationsdateien von Geräten abgerufen, die mit dem CLI-Profil erfolgreich entdeckt wurden. Nach Abschluss der Netzwerkerkennung müssen Sie die Konfigurationsverwaltung einrichten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Schnellstartsymbol für **Asset Manager**  , und wählen Sie dann die Registerkarte **Konfigurationsverwaltung** aus.
2. Führen Sie eine oder mehrere der verfügbaren Aktionen aus, und klicken Sie dann auf **OK**.

Aufgaben

- *Verwalten abgerufener Konfigurationsdateien* auf Seite 319
  Sie haben verschiedene Möglichkeiten, die Dateien zu verwalten, die bei der Überprüfung der Konfiguration von Routern und Switches abgerufen werden.

Verwalten abgerufener Konfigurationsdateien

Sie haben verschiedene Möglichkeiten, die Dateien zu verwalten, die bei der Überprüfung der Konfiguration von Routern und Switches abgerufen werden.

Bevor Sie beginnen

Rufen Sie Konfigurationsdateien ab (siehe *Einrichten der Konfigurationsverwaltung*).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Schnellstartsymbol für **Asset Manager**  , und wählen Sie dann die Registerkarte **Konfigurationsverwaltung** aus.
2. Führen Sie eine oder mehrere der verfügbaren Aktionen im Abschnitt **Abgerufene Konfigurationsdateien** der Seite aus.

Netzwerkerkennung

Unter **Netzwerkerkennung** werden die physischen Standorte im Netzwerk angezeigt, an denen Ereignisse aufgetreten sind. So können Sie Ereignisse besser verfolgen.

Die **Netzwerkerkennung** ist für fortgeschrittene Benutzer gedacht, die über umfassende Netzwerkkenntnisse verfügen. Die entsprechende Berechtigung muss zugewiesen werden. Die Berechtigungen zum Erstellen und Anzeigen der **Netzwerkerkennung** sowie zum Ändern der Switch-Einstellungen unter **Netzwerk-Port Control** müssen für Sie aktiviert sein.



Die **Netzwerkerkennung** über SNMPv3, Telnet oder SSH ist nicht FIPS-konform. Wenn Sie FIPS-Vorschriften einhalten müssen, sollten Sie diese Funktionen nicht verwenden.

Entdecken des Netzwerks

Der erste Schritt beim Zuordnen des Netzwerks besteht darin, das Netzwerk zu entdecken. Bevor Sie den Scan initiieren, müssen Sie die Parameter festlegen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Schnellstartsymbol für **Asset Manager**  , und wählen Sie dann die Registerkarte **Netzwerkerkennung** aus.
2. Klicken Sie auf **Einstellungen** und dann auf der Seite **Netzwerkeinstellungen konfigurieren** auf **Hinzufügen**, um die Parameter für diese Erkennung hinzuzufügen.
3. Füllen Sie die Einstellungen unter **Parameter für die Netzwerkerkennung** aus.
4. Klicken Sie auf **OK**. Die definierten Parameter werden zur Liste **Netzwerkeinstellungen konfigurieren** hinzugefügt.
5. Führen Sie nach Bedarf weitere Aktionen aus.
6. Klicken Sie auf **Netzwerk entdecken**, um den Scan zu initiieren. Wenn Sie die Erkennung anhalten müssen, klicken Sie auf **Erkennung anhalten**.

   Der Abschnitt **Netzwerkgerät** der Seite wird mit den Daten des Scans ausgefüllt.
7. Klicken Sie auf **OK**.

Verwalten der IP-Ausschlussliste

Wenn Sie IP-Adressen von der Suche bei der Netzwerkerkennung ausschließen möchten, können Sie diese Adressen zur **IP-Ausschlussliste** hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Schnellstartsymbol für **Asset Manager**, und wählen Sie dann die Registerkarte **Netzwerkerkennung** aus.
2. Klicken Sie auf **IP-Ausschlussliste**.
3. Fügen Sie eine neue Adresse hinzu, oder bearbeiten oder entfernen Sie eine vorhandene Adresse.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Entdecken von Endpunkten

Wenn Sie das Netzwerk einrichten, IP-Adressen zur Ausschlussliste hinzufügen und das Netzwerk entdecken, müssen Sie mit den Geräten verbundene Endpunkte entdecken.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Schnellstartsymbol für **Asset Manager**  , und wählen Sie dann die Registerkarte **Netzwerkerkennung** aus.
2. Klicken Sie auf **Endpunkte entdecken**, um den Scan sofort zu initiieren.

   Die Ergebnisse und den Status des Scans finden Sie auf der Seite im Abschnitt **Endpunktgeräte**.
3. Zum Planen der automatischen Erkennung der Endpunkte wählen Sie **Automatische Erkennung alle** und dann die Häufigkeit aus.

Anzeigen einer Netzwerkübersicht

Sie können eine grafische Darstellung des Netzwerks generieren, in der Sie die Geräte an jede gewünschte Position verschieben können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Schnellstartsymbol für **Asset Manager** und dann auf die Registerkarte **Netzwerkerkennung**.
2. Klicken Sie auf **Netzwerkübersicht**.

   Die grafische Darstellung des Netzwerks wird geöffnet.
3. Verschieben Sie Geräte, oder bewegen Sie den Mauszeiger auf ein Gerät, um die Eigenschaften anzuzeigen.

Ändern des Verhaltens der Netzwerkerkennung

Sie können die Standardeinstellungen für den Ping-Befehl, die Anzahl der Endgeräte und die gleichzeitigen Geräte für die **Netzwerkerkennung** ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf in der ESM-Konsole auf das Schnellstartsymbol für den **Asset-Manager**.
2. Klicken Sie auf die Registerkarte **Netzwerkerkennung**, auf **Einstellungen** und dann auf **Erweitert**.
3. Ändern Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **OK**.

Ressourcenquellen

Sie können gegebenenfalls Daten aus **Active Directory** oder von einem Altiris-Server mit **Ressourcenquellen** abrufen.

Mit **Active Directory** können Sie Ereignisdaten filtern, indem Sie die abgerufenen Benutzer oder Gruppen in den Abfragefilterfeldern **Quellbenutzer** oder **Zielbenutzer** für Ansichten auswählen. Auf diese Weise können Sie leichter Compliance-Daten für Anforderungen wie beispielsweise PCI bereitstellen. Ressourcen wie beispielsweise Computer mit IP-Adressen werden von Altiris und **Active Directory** abgerufen und zur Ressourcentabelle hinzugefügt.

Zum Abrufen von Ressourcen aus Altiris benötigen Sie **Asset Manager**-Berechtigungen in der Altiris-Verwaltungskonsole.

In **Active Directory** werden in der Regel keine Informationen zu IP-Adressen gespeichert. Die Adresse wird vom System über DNS abgefragt, sobald der Name aus **Active Directory** abgerufen wurde. Adressen nicht gefundener Computer werden nicht zur Tabelle **Ressourcen** hinzugefügt. Aus diesem Grund müssen sich die DNS-Informationen für **Active Directory**-Computer auf dem DNS-Server des Systems befinden.

Sie können IP-Adressen zu **Active Directory** hinzufügen. In diesem Fall ändern Sie das `networkAddress`-Attribut der Computerobjekte so, dass diese IP-Adressen anstelle einer DNS-Abfrage vom System verwendet werden.

Verwalten von Ressourcenquellen

Rufen Sie Daten aus Active Directory oder von einem Altiris-Server ab.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf das Schnellstartsymbol für **Asset Manager** und dann auf die Registerkarte **Ressourcenquellen**.

In der Struktur **Ressourcenquellen** werden das ESM-Gerät und die Empfänger im System sowie deren aktuelle Ressourcenquellen angezeigt.

Ein ESM-Gerät kann eine Ressourcenquelle haben, und Empfänger können mehrere Ressourcenquellen haben.

2 Wählen Sie ein Gerät und dann eine der verfügbaren Aktionen aus.

Verwalten von Vulnerability Assessment-Quellen

Sie können mit **Vulnerability Assessment** Daten von einer Vielzahl von VA-Anbietern abrufen. Für die Kommunikation mit den gewünschten VA-Quellen müssen Sie die jeweilige Quelle zum System hinzufügen. Wenn Sie eine Quelle zum System hinzugefügt haben, können Sie die VA-Daten abrufen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf das Schnellstartsymbol für **Asset Manager** und dann auf die Registerkarte **Vulnerability Assessment**.

2 Sie können VA-Quellen hinzufügen, bearbeiten, entfernen oder abrufen und sie dann in das Gerät schreiben.

3 Klicken Sie auf **OK**.

Zonenverwaltung

Mithilfe von Zonen können Sie Geräte und Datenquellen im Netzwerk kategorisieren.

Auf diese Weise können Sie Geräte und die von den Geräten generierten Ereignisse nach dem geographischen Standort und der IP-Adresse in verwandten Gruppen anordnen. Beispiel: Sie haben Büros in verschiedenen Landesteilen und möchten, dass die von den einzelnen Büros generierten Ereignisse gruppiert werden. Sie fügen zwei Zonen hinzu und weisen die Geräte, deren Ereignisse gruppiert werden müssen, den einzelnen Zonen zu. Zum Gruppieren der Ereignisse aus den einzelnen Büros nach bestimmten IP-Adressen fügen Sie Teilzonen zu den einzelnen Zonen hinzu.

Verwalten von Zonen

Mithilfe von Zonen können Sie Geräte und Datenquellen nach Standort (Geolocation) oder ASN kategorisieren. Fügen Sie Zonen hinzu (einzeln oder durch Importieren einer von einem anderen Computer exportierten Datei), und weisen Sie die Geräte oder Datenquellen den Zonen zu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Schnellstartsymbol für **Asset Manager**  , und wählen Sie dann **Zonenverwaltung** aus.
2. Sie können eine Zone oder Teilzone hinzufügen, vorhandene Zonen bearbeiten oder entfernen oder Zoneneinstellungen importieren oder exportieren.
3. Führen Sie einen Rollout für alle vorgenommenen Änderungen aus, und klicken Sie dann auf **OK**.

Hinzufügen einer Zone

Der erste Schritt bei der Zonenverwaltung besteht darin, die zum Kategorisieren der Geräte und Datenquellen verwendeten Zonen hinzuzufügen. Diese können Sie mit der Funktion **Zone hinzufügen** einzeln hinzufügen, oder Sie können eine von einem anderen System exportierte Datei importieren. Sie können die Einstellungen einer hinzugefügten Zone bei Bedarf bearbeiten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Schnellstartsymbol für **Asset Manager**  und dann auf **Zonenverwaltung**.
2. Geben Sie die erforderlichen Informationen ein, weisen Sie Geräte zu der Zone hinzu, und klicken Sie dann auf **OK**.

Exportieren von Zoneneinstellungen

Sie können die Zoneneinstellungen vom ESM-Gerät exportieren, um sie auf einem anderen ESM-Gerät zu importieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf das Symbol für **Asset Manager**  und dann auf **Zonenverwaltung**.
2. Klicken Sie auf **Exportieren**, und wählen Sie dann den Typ der zu exportierenden Datei aus.
3. Klicken Sie auf **OK**, und wählen Sie die Datei aus, die sofort heruntergeladen werden soll.

Importieren von Zoneneinstellungen

Mit der Importfunktion können Sie eine Zonendatei unverändert importieren oder die Daten vor dem Importieren bearbeiten.

Bevor Sie beginnen

Exportieren Sie eine Datei mit Zoneneinstellungen von einem anderen ESM-Gerät, um sie auf Ihrem ESM-Gerät zu importieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Öffnen Sie die Datei mit den Zoneneinstellungen, die Sie importieren möchten.

- Wenn es sich um eine Zonendefinitionsdatei für den Import handelt, enthält sie acht Spalten: Befehl, Zonenname, Name des übergeordneten Elements, Geolocation, ASN, Standard, IPStart und IPStop.
- Wenn es sich um eine Datei für den Import eines Geräts in eine Zonenzuweisungsdatei handelt, enthält sie drei Spalten: Befehl, Gerätename und Zonenname.

2 Geben Sie Befehle in die Spalte **Befehl** ein, um die Aktion festzulegen, die beim Import für die einzelnen Zeilen ausgeführt werden soll.

- `add` (Hinzufügen): Die Daten in der Zeile werden unverändert importiert.
- `edit` (Bearbeiten): Die Daten werden mit allen von Ihnen vorgenommenen Änderungen importiert (nur für Zonendefinitionsdateien).

  Wenn Sie Änderungen an einem Teilzonenbereich vornehmen möchten, müssen Sie den vorhandenen Bereich entfernen und dann den Bereich mit den Änderungen hinzufügen. Sie können den Bereich nicht direkt bearbeiten.

- `remove` (Entfernen): Die mit dieser Zeile übereinstimmende Zone wird vom ESM-Gerät gelöscht.

3 Speichern Sie die vorgenommenen Änderungen, und schließen Sie dann die Datei.

4 Klicken Sie auf das Schnellstartsymbol für **Asset Manager** und dann auf die Registerkarte **Zonenverwaltung**.

5 Klicken Sie auf **Importieren**, und wählen Sie dann den Typ des Imports aus.

6 Klicken Sie auf **OK**, suchen Sie dann die zu importierende Datei, und klicken Sie auf **Hochladen**.

Wenn in der Datei Fehler erkannt wurden, werden Sie vom System benachrichtigt.

7 Wenn Fehler vorhanden sind, korrigieren Sie die Datei entsprechend, und versuchen Sie es erneut.

8 Führen Sie einen Rollout für die Änderungen aus, um die Geräte zu aktualisieren.

Hinzufügen einer Teilzone

Wenn Sie eine Zone hinzugefügt haben, können Sie Teilzonen hinzufügen, um die Geräte und Ereignisse weiter nach IP-Adressen zu kategorisieren.

Bevor Sie beginnen

Fügen Sie Zonen auf der Registerkarte **Zonenverwaltung** hinzu.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf das Schnellstartsymbol für **Asset Manager** und dann auf die Registerkarte **Zonenverwaltung**.

2 Wählen Sie eine Zone aus, und klicken Sie dann auf **Teilzone hinzufügen**.

3 Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**.

Bewertung von Ressourcen, Bedrohungen und Risiken

Durch McAfee Threat Intelligence Services (MTIS) und die Quellen für Schwachstellenbewertungen im System wird eine Liste mit bekannten Bedrohungen generiert. Der Schweregrad dieser Bedrohungen und die Relevanz der einzelnen Ressourcen werden zum Berechnen der Risikostufe für Ihr Unternehmen verwendet.

Asset-Manager

Beim Hinzufügen einer Ressource zum **Asset-Manager** (siehe *Verwalten von Ressourcen*) weisen Sie eine Relevanzstufe zu. Diese Einstellung gibt an, wie wichtig die Ressource für Ihr Geschäft ist. Wenn Sie beispielsweise einen Computer zum Verwalten des Setups im Unternehmen verwenden und für diesen Computer keine Sicherung vorhanden ist, hat er eine hohe Relevanz. Wenn Sie die Einrichtung jedoch mit zwei Computern verwalten, für die jeweils eine Sicherung vorhanden ist, haben die Computer eine wesentlich niedrigere Relevanzstufe.

Sie können auswählen, ob Sie eine Ressource bei der Risikoberechnung für das Unternehmen auf der Registerkarte **Ressource** im Menü **Bearbeiten** verwenden oder ignorieren möchten.

Bedrohungsverwaltung

Auf der Registerkarte **Bedrohungsverwaltung** im **Asset-Manager** wird eine Liste mit bekannten Bedrohungen, ihrem Schweregrad und dem Anbieter angezeigt. Außerdem erfahren Sie, ob die Bedrohungen bei der Berechnung des Risikos verwendet werden. Sie können bestimmte Bedrohungen aktivieren oder deaktivieren, damit sie zum Berechnen des Risikos verwendet bzw. nicht verwendet werden. Außerdem können Sie die Details für die Bedrohungen in der Liste anzeigen. Zu diesen Details gehören Empfehlungen für den Umgang mit der Bedrohung sowie mögliche Gegenmaßnahmen.

Vordefinierte Ansichten

In drei vordefinierten Ansichten (siehe *Arbeiten mit ESM-Ansichten*) werden Daten zu Ressourcen, Bedrohungen und Risiken zusammengefasst und angezeigt:

- **Ressourcenbedrohung – Übersicht**: Zeigt die häufigsten Ressourcen nach Risikofaktor und Bedrohungsstufen nach Risiko an.
- **Aktuelle Bedrohung – Übersicht**: Zeigt aktuelle Bedrohungen nach Anbieter, Risiko, Ressource und verfügbaren Schutzprodukten an.
- **Schwachstelle – Übersicht**: Zeigt Schwachstellen nach Bedrohungen und Ressourcen an.

Auf die Details der einzelnen Elemente in diesen Ansichten können Sie über die Komponentenmenüs zugreifen.

Benutzerdefinierte Ansichten

Im **Abfragen-Assistenten** wurden Optionen hinzugefügt, mit denen Sie benutzerdefinierte Ansichten einrichten können (siehe *Hinzufügen einer benutzerdefinierten Ansicht*), in denen die benötigten Daten angezeigt werden.

- In den Komponenten **Messuhr** und **Anzahl** können Sie den durchschnittlichen Risikofaktor des Unternehmens und den Gesamtrisikofaktor des Unternehmens anzeigen.
- In den Komponenten **Kreisdiagramm**, **Balkendiagramm** und **Liste** können Sie die Ressourcen mit bestehendem Risiko, den Produktbedrohungsschutz, die Bedrohung nach Ressource, die Bedrohung nach Risiko und die Bedrohung nach Anbieter anzeigen.
- In der Komponente **Tabelle** können Sie Ressourcen, die neuesten Bedrohungen, die häufigsten Ressourcen nach Risikofaktor und die häufigsten Bedrohungen nach Risikofaktor anzeigen.

Verwalten bekannter Bedrohungen

Wählen Sie aus, welche bekannten Bedrohungen in Risikoberechnungen verwendet werden sollen.

Jede Bedrohung hat eine Bewertung des Schweregrads. Diese Bewertung und die Relevanzbewertung Ihrer Ressourcen werden zum Berechnen des Gesamtschweregrads einer Bedrohung für Ihr System verwendet.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der ESM-Konsole auf das Schnellstartsymbol für den **Asset-Manager**  .
2. Klicken Sie auf die Registerkarte **Bedrohungsverwaltung**, um die Liste mit bekannten Bedrohungen anzuzeigen.
3. Wählen Sie eine bekannte Bedrohung aus, und führen Sie dann eine der folgenden Aktionen aus:
   - Klicken Sie auf **Bedrohungsdetails**, um die Details zu der Bedrohung anzuzeigen.
   - Wenn die Spalte **Risiko berechnen** den Eintrag **Ja** enthält und die Bedrohung bei Risikoberechnungen nicht verwendet werden soll, klicken Sie auf **Deaktivieren**.
   - Wenn die Spalte **Risiko berechnen** den Eintrag **Nein** enthält und die Bedrohung bei Risikoberechnungen verwendet werden soll, klicken Sie auf **Aktivieren**.
4. Klicken Sie auf **OK**.

10 Verwalten von Richtlinien und Regeln

Sie können Richtlinienvorlagen erstellen, anwenden und anzeigen.

Inhalt

- *Grundlegendes zum Richtlinien-Editor*
- *Richtlinienstruktur*
- *Regeltypen und ihre Eigenschaften*
- *Einstellungen für Standardrichtlinien*
- *Regelvorgänge*
- *Zuweisen von Tags zu Regeln oder Ressourcen*
- *Aggregationseinstellungen ändern*
- *Überschreibungsaktion für heruntergeladene Regeln*
- *Gewichtungen der Schweregrade*
- *Anzeigen des Verlaufs der Richtlinienänderungen*
- *Anwenden von Richtlinienänderungen*
- *Verwalten von Datenverkehr mit Priorität*

Grundlegendes zum Richtlinien-Editor

Mit dem **Richtlinien-Editor** können Sie Richtlinienvorlagen erstellen und einzelne Richtlinien anpassen.

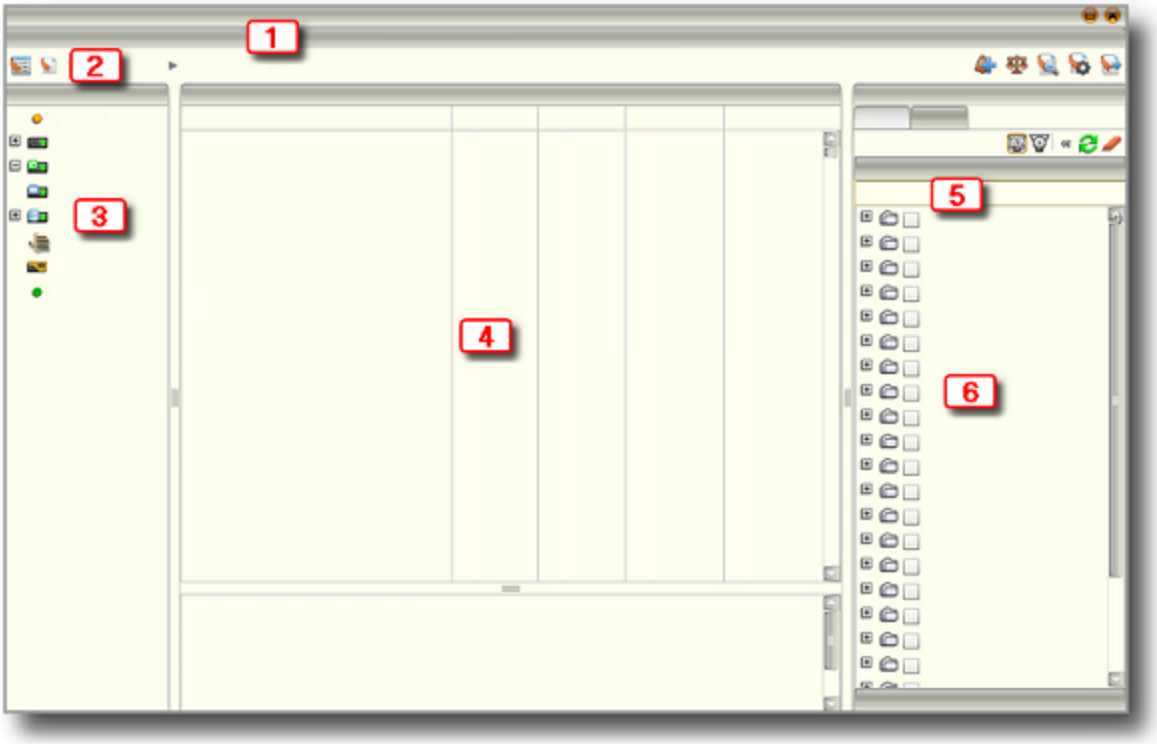
Richtlinienvorlagen können, ebenso wie Richtlinieneinstellungen auf einem Gerät, Werte von ihren übergeordneten Richtlinienvorlagen erben. Durch die Vererbung sind auf ein Gerät angewendete Richtlinieneinstellungen unbegrenzt konfigurierbar und dennoch einfach und benutzerfreundlich. Für jede hinzugefügte Richtlinie sowie für alle Geräte ist in der **Richtlinienstruktur** ein Eintrag vorhanden.



Beim Betrieb im FIPS-Modus sollten Sie die Regeln nicht über den Regel-Server aktualisieren. Aktualisieren Sie sie stattdessen manuell (siehe *Überprüfen auf Regelaktualisierungen*).

Auf dem McAfee-Regel-Server werden alle Regeln, Variablen und Präprozessoren mit vordefinierten Werten oder Verwendungen verwaltet. Die **Standardrichtlinie** erbt ihre Werte und Einstellungen von diesen von McAfee verwalteten Einstellungen, und alle anderen Richtlinien erben von ihr. Einstellungen für alle anderen Richtlinien und Geräte erben standardmäßig ihre Werte von der **Standardrichtlinie**.

Zum Öffnen des Editors klicken Sie auf das Symbol **Richtlinien-Editor**, oder wählen Sie das System oder den Geräteknoten in der Navigationsstruktur aus, und klicken Sie auf der Aktionssymbolleiste auf das Symbol **Richtlinien-Editor**  .



1	Menüleiste	4	Regelanzeige
2	Navigationsbereich	5	Suchfeld für Tags
3	Bereich für Regeltypen	6	Bereich Filter/Kennzeichnung

Die im Bereich **Regeltypen** aufgeführten Regeltypen hängen davon ab, welcher Gerätetyp in der Systemnavigationsstruktur ausgewählt ist. Im Navigationsbereich wird die Hierarchie der ausgewählten Richtlinie angezeigt. Zum Ändern der aktuellen Richtlinie klicken Sie im Navigationsbereich auf den Namen der Richtlinie und auf den Pfeil. Daraufhin werden die untergeordneten Elemente der Richtlinie angezeigt. Alternativ können Sie auf das Symbol **Richtlinienstruktur** klicken. Im Menü **Richtlinienstruktur** werden die Aktionen aufgeführt, die Sie für eine Richtlinie ausführen können.

Wenn Sie im Bereich **Regeltypen** einen Typ auswählen, werden im Abschnitt Regelanzeige alle Regeln dieses Typs aufgeführt. Die Spalten enthalten die spezifischen Regelparameter, die Sie für die jeweilige Regel anpassen können (mit Ausnahme von **Variable** und **Präprozessor**). Sie können die Einstellungen ändern, indem Sie auf die aktuelle Einstellung klicken und in der Dropdown-Liste eine neue Einstellung auswählen.

Im Bereich **Filter/Kennzeichnung** können Sie die im **Richtlinien-Editor** angezeigten Regeln filtern. Auf diese Weise können Sie nur die Ihren Kriterien entsprechenden Regeln anzeigen oder Tags zu den Regeln hinzufügen, um ihre Funktionen zu definieren.

Richtlinienstruktur

In der **Richtlinienstruktur** werden die Richtlinien und Geräte im System aufgeführt.

In der **Richtlinienstruktur** haben Sie folgende Möglichkeiten:

- Navigieren, um die Details einer bestimmten Richtlinie oder eines bestimmten Geräts anzuzeigen
- Hinzufügen einer Richtlinie zum System
- Ändern der Reihenfolge der Richtlinien oder Geräte
- Suchen einer Richtlinie oder eines Geräts anhand des Namens
- Umbenennen, Löschen, Kopieren bzw. Kopieren und Ersetzen, Importieren oder Exportieren einer Richtlinie

Symbol	Beschreibung
	Richtlinie
	Das Gerät ist nicht synchronisiert.
	Das Gerät ist bereitgestellt.
	Das Gerät ist aktuell.
	Das virtuelle Gerät ist nicht synchronisiert.
	Das virtuelle Gerät ist bereitgestellt.
	Das virtuelle Gerät ist aktuell.
	Die Datenquelle ist nicht synchronisiert.
	Die Datenquelle ist bereitgestellt.
	Die Datenquelle ist aktuell.
	Das ADM-Gerät ist nicht synchronisiert.
	Das DEM-Gerät ist nicht synchronisiert.

Verwalten von Richtlinien in der Richtlinienstruktur

Verwalten Sie die Richtlinien im System, indem Sie in der **Richtlinienstruktur** Aktionen ausführen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ESM-Konsole auf das Symbol **Richtlinien-Editor**  und dann auf das Symbol **Richtlinienstruktur**  .

2 Führen Sie eine oder mehrere der folgenden Aktionen aus:

Aufgabe	Vorgehensweise
Anzeigen der Regeln einer Richtlinie	• Doppelklicken Sie auf die Richtlinie. Die Regeln werden im **Richtlinien-Editor** im Abschnitt Regelanzeige aufgeführt.
Festlegen einer Richtlinie als untergeordnetes Element einer anderen Richtlinie	• Wählen Sie das untergeordnete Element aus, ziehen Sie es auf das übergeordnete Element, und legen Sie es dort ab. Sie können nur Geräte auf Richtlinien ziehen und dort ablegen.
Suchen einer Richtlinie oder eines Geräts	• Geben Sie den Namen in das Suchfeld ein.

Aufgabe	Vorgehensweise
Hinzufügen einer neuen Richtlinie	1 Wählen Sie die Richtlinie aus, zu der Sie eine neue Richtlinie hinzufügen möchten, und klicken Sie dann auf das Symbol **Menüelemente der Richtlinienstruktur**  . 2 Klicken Sie auf **Neu**, geben Sie einen Namen für die Richtlinie ein, und klicken Sie dann auf **OK**.
Umbenennen einer Richtlinie	1 Wählen Sie die umzubenennende Richtlinie aus, und klicken Sie dann auf das Symbol **Menüelemente der Richtlinienstruktur**. 2 Klicken Sie auf **Umbenennen**, geben Sie den neuen Namen ein, und klicken Sie dann auf **OK**.
Löschen einer Richtlinie	1 Wählen Sie die zu löschende Richtlinie aus, und klicken Sie dann auf das Symbol **Menüelemente der Richtlinienstruktur**. 2 Klicken Sie auf **Löschen** und dann auf der Bestätigungsseite auf **OK**.
Kopieren einer Richtlinie	1 Wählen Sie die zu kopierende Richtlinie aus, und klicken Sie dann auf das Symbol **Menüelemente der Richtlinienstruktur**. 2 Klicken Sie auf **Kopieren**, geben Sie einen Namen für die neue Richtlinie ein, und klicken Sie dann auf **OK**.
Verschieben von Geräten in eine Richtlinie	1 Wählen Sie die zu verschiebenden Geräte aus, und klicken Sie dann auf das Symbol **Menüelemente der Richtlinienstruktur**  . 2 Heben Sie **Verschieben** hervor, und wählen Sie dann die Richtlinie aus, in die Sie die Geräte verschieben möchten.
Kopieren und Ersetzen einer Richtlinie	1 Wählen Sie die zu kopierende Richtlinie aus, klicken Sie auf das Symbol **Menüelemente der Richtlinienstruktur**, und wählen Sie dann **Kopieren und ersetzen** aus. 2 Wählen Sie in **Richtlinie auswählen** die Richtlinie aus, die Sie ersetzen möchten. 3 Klicken Sie auf **OK** und dann auf **Ja**. Die Einstellungen der kopierten Richtlinie werden auf die ersetzte Richtlinie angewendet. Der Name bleibt jedoch gleich.

Aufgabe	Vorgehensweise
Importieren einer Richtlinie	Der Import wird für das zurzeit ausgewählte Gerät und die darunter angeordneten Geräte ausgeführt. 1 Wählen Sie in der Struktur die Ebene aus, auf der Sie die neue Richtlinie importieren möchten, klicken Sie auf das Symbol **Menüelemente der Richtlinienstruktur**, und wählen Sie dann **Importieren** aus. 2 Navigieren Sie zu der zu importierenden Datei, und laden Sie sie hoch. Wenn eine Fehlermeldung angezeigt wird, finden Sie unter Fehlerbehebung im Abschnitt *Importieren einer Richtlinie* eine Lösung. 3 Wählen Sie die gewünschten Importoptionen aus, und klicken Sie dann auf **OK**.
Exportieren einer Richtlinie	1 Wählen Sie die Richtlinie aus, die Sie exportieren möchten. Der Export enthält den ausgewählten Knoten und alle in der Hierarchie darüber liegenden Knoten. Da nur Standardregeln mit benutzerdefinierten Einstellungen oder benutzerdefinierte Regeln exportiert werden, muss mindestens eine dieser Regeln ausgewählt sein, damit die Option **Exportieren** aktiviert wird. 2 Klicken Sie auf **Menü**, und wählen Sie dann **Exportieren** aus. 3 Wählen Sie die gewünschten Exportoptionen aus, klicken Sie auf **OK**, und wählen Sie dann den Speicherort für die exportierte Richtliniendatei aus.

3 Zum Schließen der **Richtlinienstruktur** doppelklicken Sie auf eine Richtlinie oder ein Gerät, oder klicken Sie auf das Symbol zum Schließen .

Regeltypen und ihre Eigenschaften

Im Bereich **Regeltypen** der Seite **Richtlinien-Editor** können Sie auf alle Regeln nach dem Typ zugreifen.

Sie können eine ausgewählte Regel importieren, exportieren, hinzufügen und bearbeiten und verschiedene Vorgänge für die Regel ausführen. Welche Funktionen Sie ausführen können, hängt vom Typ der Regel ab.

Alle Regeln basieren auf einem Hierarchiesystem, in dem jede Regel ihre Verwendung von der jeweils übergeordneten Regel erbt. Die Regel (mit Ausnahme von **Variablenregeln** und **Präprozessorregeln**) wird mit einem Symbol markiert, aus dem hervorgeht, von welchem Element sie die Verwendung erbt. Wenn die Vererbungskette an einer beliebigen Stelle unterhalb der aktuellen Zeile unterbrochen wurde, ist das Symbol mit einem Punkt in der linken unteren Ecke versehen.

Symbol	Beschreibung
	Weist darauf hin, dass die Verwendung dieses Elements durch die Einstellung des übergeordneten Elements bestimmt wird. Für die meisten Regeln ist standardmäßig die Vererbung festgelegt, die Verwendung kann jedoch geändert werden.
	Weist darauf hin, dass die Vererbungskette auf dieser Ebene unterbrochen ist und der Wert für die Vererbung deaktiviert ist. Wenn die Vererbungskette unterbrochen ist, wird die aktuelle Regelverwendung verwendet.

Symbol	Beschreibung
	Gibt an, dass die Vererbung auf dieser Ebene unterbrochen ist. Elemente unterhalb dieser Stelle erben keine Einstellungen von weiter oben in der Kette angeordneten Elementen. Diese Einstellung ist hilfreich, wenn Sie die Verwendung der Standardwerte für Regeln erzwingen möchten.
	Gibt einen benutzerdefinierten Wert an, den Sie auf einen anderen als den Standardwert festlegen.

Eigenschaften

Wenn ein Regeltyp ausgewählt ist, werden im Regelanzeigebereich alle im System vorhandenen Regeln dieses Typs und ihre Eigenschaftseinstellungen angezeigt. Möglich sind die Eigenschaften **Aktion**, **Schweregrad**, **Blacklist**, **Aggregation** und **Paket kopieren**.

Eigenschaft	Zweck
Aktion	Legen Sie die von dieser Regel ausgeführte Aktion fest. Die verfügbaren Optionen basieren auf dem Typ der Regel. Blacklist-Elemente können nicht an ihre Ziele verschoben werden. Wenn in der Spalte **Blacklist** die Option **Zulassen** ausgewählt ist, wird die Option vom System automatisch in **Warnung** geändert.
Schweregrad	Wählen Sie den Schweregrad des Regelabschnitts bei Auslösung der Regel aus. Der Schweregrad wird mit 1 bis 100 angegeben, wobei 100 dem höchsten Schweregrad entspricht.
Blacklist	Wenn die Regel auf dem Gerät ausgelöst wird, wird automatisch ein Blacklist-Eintrag pro Regel erstellt. Sie können auswählen, ob nur die IP-Adresse oder die IP-Adresse und der Port in die Blacklist aufgenommen werden sollen.
Aggregation	Legen Sie die Aggregation pro Regel für Ereignisse fest, die bei Auslösung einer Regel erstellt werden. Die auf der Seite **Ereignisaggregation** definierten Aggregationseinstellungen (siehe *Aggregieren von Ereignissen oder Flüssen*) gelten nur für die im Richtlinien-Editor festgelegten Regeln.
Paket kopieren	Kopieren Sie Paketdaten auf das ESM-Gerät. Dies ist hilfreich beim Verlust der Kommunikation. Wenn eine Kopie der Paketdaten vorhanden ist, können Sie auf die Informationen zugreifen, indem Sie die Kopie abrufen.

Sie können diese Einstellung ändern, indem Sie auf die aktuelle Einstellung klicken und eine andere auswählen.

Variablen

Eine *Variable* ist eine globale Einstellung oder ein Platzhalter für Benutzer- oder Site-spezifische Informationen. Variablen werden in vielen Regeln verwendet.

Wenn Sie Variablen hinzufügen oder ändern möchten, sollten Sie über umfassende Kenntnisse des Snort-Formats verfügen.

Variablen werden verwendet, um ein bestimmtes Verhalten von Regeln zu erreichen, das je nach Gerät unterschiedlich sein kann. Das ESM-Gerät verfügt über zahlreiche vordefinierte Variablen. Sie können jedoch auch benutzerdefinierte Variablen hinzufügen. Beim Hinzufügen einer Regel werden diese Variablen als Optionen in der Dropdown-Liste für den Feldtyp angezeigt, den Sie auf der Seite **Neue Variable** im Feld **Typ** festgelegt haben.

Jede Variable hat einen Standardwert, es wird jedoch empfohlen, Werte festzulegen, die der spezifischen Umgebung des jeweiligen Geräts entsprechen. Leerzeichen sind beim Eingeben eines Variablennamens nicht zulässig. Wenn Sie ein Leerzeichen benötigen, verwenden Sie das Zeichen für den Unterstrich (_). Damit Sie ein Gerät möglichst effizient nutzen können, müssen Sie insbesondere die Variable HOME_NET auf das Heimnetzwerk festlegen, das mit dem jeweiligen Gerät geschützt wird.

In dieser Tabelle finden Sie eine Liste mit gängigen Variablen und den zugehörigen Standardwerten.

Variablennamen	Beschreibung	Standardwert	Standardbeschreibung
EXTERNAL_NET	Jeder außerhalb des geschützten Netzwerks	!$HOME_NET	Port 80
HOME_NET	Lokal geschützter Netzwerk-Adressbereich (10.0.0.0/80)	Alle	Wie HOME_NET
HTTP_PORTS	Web-Server-Ports: 80 oder 80:90 für einen Bereich zwischen 80 und 90	80	Alle Ports mit Ausnahme von HTTP_PORTS
HTTP_SERVERS	Adressen von Web-Servern: 192.168.15.4 oder [192.168.15.4,172.16.61.5]	$HOME_NET	Wie HOME_NET
SHELLCODE_PORTS	Alles außer Web-Server-Ports	!$HTTP_PORTS	Wie HOME_NET
SMTP	Adressen von E-Mail-Servern	$HOME_NET	Wie HOME_NET
SMTP_SERVERS	Adressen von E-Mail-Servern	$HOME_NET	Wie HOME_NET
SQL_SERVERS	Adressen von SQL-Datenbank-Servern	$HOME_NET	Wie HOME_NET
TELNET_SERVERS	Adressen von Telnet-Servern	$HOME_NET	Wie HOME_NET

Im Lieferumfang des Systems enthaltene Variablen können geändert werden. Benutzerdefinierte Variablen können hinzugefügt, geändert oder gelöscht werden.

Sie können benutzerdefinierten Variablen Typen zuweisen. Mithilfe von Variablentypen können Sie beim Filtern von Regeln für die Berichterstellung das Feld bestimmen, in dem die Variablen beim Hinzufügen oder Ändern einer Regel zur Verfügung stehen. Variablentypen sind von Natur aus global. Alle Änderungen gelten auf allen Ebenen der Richtlinie.

Verwalten von Variablen

Wenn Sie im **Richtlinien-Editor** den Regeltyp Variable auswählen, können Sie verschiedene Aktionen ausführen, um benutzerdefinierte und vordefinierte Variablen zu verwalten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf das Symbol **Richtlinien-Editor**.

2 Wählen Sie im Bereich **Regeltypen** die Option **Variable** aus.

3 Führen Sie einen oder mehrere der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Hinzufügen einer neuen Kategorie	1 Wählen Sie Folgendes aus: **Neu** | **Kategorie**. 2 Geben Sie einen Namen für die neue Kategorie ein, und klicken Sie dann auf **OK**.
Hinzufügen einer neuen benutzerdefinierten Variablen	1 Wählen Sie im Regelanzeigebereich die Kategorie aus, und klicken Sie dann auf **Neu**. 2 Wählen Sie **Variable** aus, und definieren Sie dann die erforderlichen Einstellungen. 3 Klicken Sie auf **OK**.
Ändern einer Variablen	1 Wählen Sie im Regelanzeigebereich die Variable aus, die Sie ändern möchten. 2 Wählen Sie **Bearbeiten** aus, und klicken Sie dann auf **Ändern**. 3 Ändern Sie den Wert oder die Beschreibung, und klicken Sie dann auf **OK**.
Löschen einer benutzerdefinierten Variablen	1 Wählen Sie im Regelanzeigebereich die Variable aus, die Sie entfernen möchten. 2 Wählen Sie **Bearbeiten** aus, und klicken Sie dann auf **Löschen**.
Importieren einer Variablen	1 Wählen Sie **Datei** aus, und klicken Sie dann auf **Importieren** | **Variablen**. 2 Klicken Sie auf **Importieren**, navigieren Sie zu der Datei, und laden Sie sie hoch. Bei der Importdatei muss es sich um eine TXT-Datei handeln, die die folgenden Informationen in diesem Format enthält: Variablenname;Variablenwert; Kategoriename (optional); Beschreibung (optional). Wenn ein Feld fehlt, muss als Platzhalter ein Semikolon verwendet werden.
Ändern des Typs einer benutzerdefinierten Variablen	1 Wählen Sie die benutzerdefinierte Variable aus. 2 Klicken Sie auf **Bearbeiten**, und wählen Sie dann **Ändern** aus. 3 Ändern Sie den Variablentyp. Wenn der Variablentyp auf eine andere Option als **Kein Typ ausgewählt** festgelegt ist und diese Einstellung angewendet wurde, können Sie den Wert nicht ändern. 4 Klicken Sie auf **OK**, um die Änderungen zu speichern.

Entdecken von TCP-Protokollanomalien und Übernahme der Kontrolle über TCP-Sitzungen

Sie können TCP-Protokollanomalien entdecken und entsprechende Warnungen ausgeben und auf Übernahmen der Kontrolle über TCP-Sitzungen überprüfen, indem Sie die Stream5-Präprozessor-Variable verwenden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der ESM-Konsole auf das Symbol **Richtlinien-Editor** .
2. Klicken Sie im Bereich **Regeltypen** auf **Variable**.
3. Klicken Sie im Regelanzeigebereich auf **Präprozessor**, und wählen Sie dann **STREAM5_TCP_PARAMS** aus.
4. Fügen Sie auf der Seite **Variable ändern** im Feld **Wert** einen der folgenden Werte hinzu:
   - Fügen Sie `detect_anomalies` nach **policy first** hinzu, um TCP-Protokollanomalien zu entdecken und entsprechende Warnungen auszugeben.
   - Fügen Sie `detect_anomalies check_session_hijacking` nach **policy first** hinzu, um auf Übernahmen der Kontrolle über TCP-Sitzungen zu überprüfen.

Präprozessorregeln

Mit Präprozessoren können Sie die Entdeckung von Anomalien und die Überprüfung von Paketen in McAfee Nitro IPS und IDS vereinheitlichen.

Präprozessoren sind für die genaue Entdeckung vieler Regeln unerlässlich. Verwenden Sie die Ihrer Netzwerkkonfiguration entsprechenden Präprozessoren. Sie können die Parameter für die Präprozessoren ändern, indem Sie die entsprechende Präprozessor-Variable im **Richtlinien-Editor** unter dem Regeltyp **Variablen** bearbeiten.

Typ	Beschreibung
RPC-Normalisierung	Normalisiert für das RPC-Protokoll spezifischen Datenverkehr nur zu Entdeckungszwecken auf einheitliche Weise. Mit diesem Präprozessor können Sie verhindern, dass das Nitro IPS-Gerät bei Angriffen im Zusammenhang mit RPC-Fragmentierung umgangen wird.
Entdeckung von Port-Scans	Generiert ein Ereignis, wenn ein Port-Scan auf den Geräten auf der vertrauenswürdigen Seite des Netzwerks entdeckt wird. Wenn Sie die Variable HOME_NET richtig festgelegt haben, sollten Sie die Variable SFPORTSCAN_PARMS (Variablen | Präprozessor) wie folgt ändern: `proto { all } scan_type { all } sense_level { medium } ignore _scanners` Diese Zeichenfolge wird zu der Variable sfportscan hinzugefügt, um die vom Nitro IPS-Gerät erkannten Port-Scans aus dem Heimnetzwerk (HOME_NET) zu eliminieren. In Netzwerken, in denen sich das Nitro IPS- oder IDS-Gerät in der Nähe eines Routers oder einer Firewall mit Netzwerkadressübersetzung (Network Address Translation, NAT) befindet, wird scheinbar ein Port-Scan auf dem Nitro IPS-Gerät ausgeführt. Durch das Ändern der Variablen verringern Sie die Anzahl der mutmaßlichen False-Positive-Ereignisse. Damit ignore_scanners richtig funktioniert, darf HOME_NET nicht auf "any" festgelegt sein.
ZipZap	Beim Bereitstellen von Web-Inhalten (HTTP) werden von vielen Web-Servern Anfragen von Web-Browsern akzeptiert, bei denen darauf hingewiesen wird, dass der Web-Inhalt vor dem Senden komprimiert werden kann. Dadurch wird zwar Bandbreite im Netzwerk gespart, jedoch können die komprimierten Web-Seiten von einem Gerät nicht analysiert werden. Der ZipZap-Präprozessor bewirkt, dass diese Daten vom Web-Server in einem unbearbeiteten, nicht komprimierten und analysierbaren Format zurückgegeben werden. Wenn Sie diesen Präprozessor aktivieren, erhöht sich die Menge der für Web-Verkehr genutzten Bandbreite.

Typ	Beschreibung
Zielbasierte IP-Defragmentierung	Modelliert die eigentlichen Ziele im Netzwerk, anstatt lediglich die Protokolle zu modellieren und nach Angriffen innerhalb dieser Protokolle zu suchen. Mithilfe der sfxhash-Datenstruktur und der verknüpften Listen werden die Daten intern verarbeitet. Dadurch wird eine vorhersehbare und deterministische Leistung in allen Umgebungen ermöglicht, sodass stark fragmentierte Umgebungen leichter verwaltet werden können.
Normalisierung von Web-Anfragen	Normalisiert Web-Anfragen nur zu Entdeckungszwecken auf einheitliche Weise. Der Präprozessor ist immer aktiviert, Sie können jedoch keine Änderungen vornehmen. Es gibt zwei Arten von Präprozessoren für die Normalisierung von Web-Anfragen: einen für die Verwendung mit Versionen bis 8.2.X und einen für Version 8.3.0 und höher. Durch diesen Präprozessor werden die folgenden Angriffe entdeckt: • Angriffe mit Web-Verzeichnisdurchquerung (http://Beispiel.com/./Angriff.cmd) • Doppelt codierte Zeichenfolgen (http://Beispiel.com/%25%32%35%25%33%32%25%33%30Angriff.cmd) • Unicode-Normalisierung • Ungültige Zeichen in einem Web-Anfrage-URI
Zielbasiertes Zusammensetzen von TCP-Datenströmen und Überwachung von TCP- und UDP-Sitzungen	Verfolgt Sitzungen. Da es sich um einen Stream5-Präprozessor handelt, können die Regelstichwörter rule flow und flow bits für TCP- und UDP-Datenverkehr verwendet werden.

Verwalten von Präprozessorregeln

Aktivieren oder deaktivieren Sie die einzelnen Präprozessoren, und legen Sie die Vererbung fest.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im **Richtlinien-Editor** im Bereich **Regeltypen** auf **IPS** | **Präprozessor**.

2 Wählen Sie für die aktiven Regeln die Option **Vererben**, **An** oder **Aus** aus.

Firewall-Regeln

Firewall-Regeln werden verwendet, um auf einem Nitro IPS-Gerät Netzwerkereignisse basierend auf Paketinformationen wie beispielsweise Protokoll, Port oder IP-Adresse zu entdecken.

Mit der Firewall-Richtlinie werden eingehende Pakete gescannt und Entscheidungen getroffen, die auf anfänglichen Informationen basieren. Diese werden gefunden, bevor das Paket dem Deep Packet Inspection-Modul übergeben wird. Durch Firewall-Regeln werden beispielsweise gefälschte und ungültige IP-Adressen blockiert. Außerdem werden Rate und Größe des Netzwerkverkehrs verfolgt.

Die folgenden Firewall-Regeltypen stehen zur Verfügung:

- **Anomalie**: Entdeckt Anomalien. Viele auf Anomalien basierende Regeln sind deckungsgleich und werden mit den auf der Registerkarte **Variablen** festgelegten Werten verwendet. Beispielsweise werden die Regel **Long Connection Duration** (Verbindung mit langer Dauer) und die Variable **Long Duration Seconds** (Verbindung mit langer Dauer in Sekunden) gemeinsam verwendet, um die Anzahl der Sekunden bis zum Auslösen der Regel zu ermitteln. Konkretere Details zu den einzelnen Regeln finden Sie unten auf der Seite in dem Detailabschnitt.
- **Schutz vor Spoofing**: Entdeckt ungültige IP-Adressen. Die Regel für den Schutz vor Spoofing wird beispielsweise ausgelöst, wenn eine reservierte interne IP-Adresse als über ein Gerät im Netzwerk eingehende IP-Adresse beobachtet wird.
- **Blacklist**: Bestimmt die Aktion, die für Pakete ausgeführt werden soll, die von bzw. an IP-Adressen oder Ports in der Blacklist gesendet werden.
- **DHCP**: Aktiviert oder deaktiviert die Möglichkeit, DHCP-Verkehr durch ein Gerät zuzulassen.
- **IPv6**: Entdeckt IPv6-Verkehr.
- **Port-Blockierung**: Blockiert bestimmte Ports.

Entdeckung von Anomalien

Bestimmte Firewall-Regeln basieren auf Raten. Eine *ratenbasierte Regel* löst nur dann eine Warnung aus, wenn der Netzwerkverkehr die Schwellenwerte überschreitet, die Sie mit Variablen aus der Firewall-Kategorie im **Richtlinien-Editor** definiert haben. Die Standardwerte für diese Variablen müssen für Ihren Netzwerkverkehr nicht zwangsläufig sinnvoll sein. Daher haben Sie im **Assistenten zur Entdeckung von ratenbasierten Anomalien** die Möglichkeit, Diagramme der Netzwerk-Flussdaten in Bezug auf diese Parameter zu analysieren (siehe *Assistent zur Entdeckung von Anomalien*).

Firewall-Ausnahmen

Firewall-Ausnahmen sind manchmal notwendig, wenn Sie zulassen möchten, dass bestimmte Verkehrstypen, die ansonsten blockiert würden, die Firewall passieren. Wenn beispielsweise eine gültige interne Adresse von einem externen Netzwerk (z. B. einem VPN) kommt, wird eine Warnung zu eingehenden Bogons ausgelöst. Um die Warnung zu verhindern, müssen Sie eine Ausnahme für die Firewall-Regel einrichten.

Sie können auch auswählen, dass eine Ausnahme als Ausnahme von den in anderen Ausnahmen definierten Mustern behandelt werden soll. Dabei erstellen Sie eine Ausnahme für die Ausnahmeliste (mit anderen Worten: Sie fügen eine Adresse oder einen Adressblock hinzu). Wenn eine Adresse anhand einer Firewall-Regel überprüft werden muss und die IP-Adresse in einem bereits akzeptierten Adressblock enthalten ist, können Sie die Adresse von der Ausnahmeliste ausschließen. Dazu geben Sie die IP-Adresse (oder Maske) ein und wählen das Feld aus.

Beispiel: Die Ausnahmeliste enthält bereits den Adressblock 10.0.0.0/24. Alle Adressen in diesem Bereich stellen eine Ausnahme von der Regel dar. Wenn für diese Regel die Quelladresse 10.0.0.1 aktiv ist, wählen Sie **Als Ausnahme zu den in anderen Ausnahmen definierten Mustern behandeln** aus, und geben Sie 10.0.0.1 in das Quellfeld ein. Die Firewall-Regel gilt dann für 10.0.0.1, aber nicht für andere Adressen im Block 10.0.0.0/24, da 10.0.0.1 jetzt die Ausnahme von der Ausnahmeliste ist.

Hinzufügen einer benutzerdefinierten Firewall-Regel

Normalerweise reichen die Firewall-Standardregeln aus, um das Netzwerk zu schützen. Es kann jedoch Fälle geben, in denen Sie spezielle Regeln für ein geschütztes System oder eine geschützte Umgebung hinzufügen müssen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** Folgendes aus: **IPS** | **Firewall**.

2 Wählen Sie **Neu** aus, und klicken Sie dann auf **Firewall-Regel**.

3 Definieren Sie die Einstellungen, und klicken Sie dann auf **OK**.

Die Filter in der neuen Regel werden angewendet, und die neue Regel wird im Regelanzeigebereich angezeigt. Wenn Sie auf das Filtersymbol klicken, werden die Filter gelöscht.

Hinzufügen von Firewall-Ausnahmen

Fügen Sie Ausnahmen zu Firewall-Regeln hinzu, um zuzulassen, dass Netzwerkereignisse von festgelegten Protokollen, IP-Adressen oder Ports die Firewall passieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** Folgendes aus: **IPS** | **Firewall**.

2 Klicken Sie im Regelanzeigebereich auf die Regel, für die Sie eine Ausnahme hinzufügen möchten.

Sie können die Regel leichter finden, wenn Sie die Filter im Bereich **Filter/Kennzeichnung** verwenden (siehe *Filterregeln*).

3 Wählen Sie **Neu** aus, und klicken Sie dann auf **Firewall-Ausnahme**.

4 Klicken Sie auf **Hinzufügen**, und wählen Sie dann die Werte zum Definieren der Ausnahme aus, oder geben Sie sie ein.

5 Klicken Sie auf **OK**.

Deep Packet Inspection-Regeln

Mit Deep Packet Inspection-Regeln können Sie den Inhalt eines Pakets testen und mit Mustern in den Regelsignaturen vergleichen. Wenn eine Übereinstimmung vorliegt, wird die angegebene Aktion ausgeführt.

Der BASE-Filter (im Bereich **Filter/Kennzeichnung**) bietet Schutz vor bekannten Eindringungsversuchen, die schädlich für das System oder dessen Daten sein können. Das gleiche gilt für die Filter MALWARE und VIRUS. Mit den Filtern RICHTLINIE und MULTIMEDIA können Sie Netzwerkaktivitäten im Zusammenhang mit benutzerdefinierten Angaben für die Netzwerkverwendung verhindern oder entsprechende Warnungen ausgeben. Diese Filter sind nicht potenziell gefährlichen Netzwerk-Eindringungsversuchen zugeordnet. Es gibt die folgenden allgemeinen Filtergruppentypen:

- Schutzregeln (BASE, MALWARE, PERIMETER, VIRUS)
- Richtlinienregeln (CHAT, MULTIMEDIA, PEERTOPEER, RICHTLINIE, SECURE APPLICATION GATEWAY)

Normalerweise reichen die Standardregeln aus, um das Netzwerk zu schützen. Es kann jedoch Fälle geben, in denen spezielle Regeln für ein geschütztes System oder eine geschützte Umgebung erforderlich sind. Sie können benutzerdefinierte Deep Packet Inspection-Regeln zum ESM-Gerät hinzufügen (siehe *Hinzufügen von Deep Packet Inspection-Regeln*).

Hinzufügen von Deep Packet Inspection-Regeln

Fügen Sie eine benutzerdefinierte Deep Packet Inspection-Regel hinzu, wenn Sie diese für ein geschütztes System oder eine geschützte Umgebung benötigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie im **Richtlinien-Editor** Folgendes aus: **Nitro IPS** | **Deep Packet Inspection**.
2. Klicken Sie auf **Neu**, und wählen Sie dann **Deep Packet Inspection-Regel** aus.
3. Definieren Sie die Einstellungen, und klicken Sie dann auf **OK**.

Die Filter in der neuen Regel werden angewendet, und die neue Regel wird im Regelanzeigebereich angezeigt. Wenn Sie auf das Filtersymbol klicken, werden die Filter gelöscht, und alle Deep Packet Inspection-Regeln werden angezeigt.

Hinzufügen eines Deep Packet Inspection-Attributs

Wenn Sie eine Deep Packet Inspection-Regel hinzufügen oder bearbeiten, müssen Sie unter anderem der Regel Attribute zuweisen. Mit diesen Attributen definieren Sie die Aktion für die Regel. Sie können in der Liste benutzerdefinierte Optionen hinzufügen und löschen, die einer Regel zugewiesen werden können.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie im **Richtlinien-Editor** Folgendes aus: **IPS** | **Deep Packet Inspection** | **Hinzufügen**.
2. Wählen Sie in der Dropdown-Liste die Kategorie für das Attribut aus.
3. Wählen Sie im Feld **Optionen** die dem Attribut zugeordnete Aktion aus.
4. Geben Sie einen Wert für die ausgewählte Option ein, und klicken Sie dann auf **OK**.

Der Wert und der Name der Option werden zur Tabelle **Regeloptionen** hinzugefügt. Wählen Sie den Wert aus, um ihn zu bearbeiten oder zu löschen.

Interne Regeln

Der Regeltyp **Intern** enthält Regeln mit Signatur-IDs zwischen 3.000.000 und 3.999.999. Dabei handelt es sich um interne Warnungen, die im Gegensatz zu anderen Regeln nicht über Signaturen verfügen. Diese Regeln können nur aktiviert oder deaktiviert werden.

Dieser Regeltyp ist nur verfügbar, wenn in der Systemnavigationsstruktur ein Nitro IPS-Gerät oder ein virtuelles Gerät ausgewählt ist.

Verwalten interner Regeln

Zeigen Sie die Liste der vorhandenen internen Regeln an, oder ändern Sie den Status dieser Regeln.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie in der Systemnavigationsstruktur ein Nitro IPS-Gerät oder ein virtuelles Gerät aus.
2. Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** Folgendes aus: **IPS** | **Intern**.
3. Klicken Sie in der Spalte **Aktivieren** auf **Alles auswählen** oder auf **Nichts auswählen**, oder wählen Sie einzelne Regeln aus, bzw. heben Sie die Auswahl einzelner Regeln auf.

Filterregeln

Mit Filterregeln können Sie festlegen, welche Aktion ausgeführt werden soll, wenn von Ihnen definierte Daten beim Empfänger eingehen.

Datenreihenfolge

Filterregeln werden in der folgenden Datenreihenfolge in den Empfänger geschrieben:

1. Alle Regeln außer Erfassungsregeln
   a. Anhalten = wahr und Analysieren = falsch und Protokollieren = falsch
   b. Anhalten = wahr und Analysieren = wahr und Protokollieren = wahr
   c. Anhalten = wahr und Analysieren = wahr und Protokollieren = falsch
   d. Anhalten = wahr und Analysieren = falsch und Protokollieren = wahr
2. Alle Erfassungsregeln

Regelreihenfolge

Wenn Sie über Rechte als **Richtlinienadministrator** verfügen, können Sie die Reihenfolge definieren, in der die Filterregeln ausgeführt werden sollen. Diese Regeln werden dann in der Reihenfolge ausgeführt, mit der Sie die benötigten Daten auf die effizienteste Weise erhalten (siehe *Festlegen der Reihenfolge für ASP-Regeln und Filterregeln*).

Hinzufügen von Filterregeln

Sie können Filterregeln zum **Richtlinien-Editor** hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie im **Richtlinien-Editor** Folgendes aus: **Empfänger** | **Filter**.
2. Wählen Sie **Neu** aus, und klicken Sie dann auf **Filterregel**.
3. Füllen Sie die Felder aus, und klicken Sie dann auf **OK**
4. Zum Aktivieren der Regel wählen Sie die Regel im Regelanzeigebereich aus, klicken Sie in der Spalte **Aktion** auf die Einstellung, und klicken Sie dann auf **aktiviert**.

ASP-Regeln

Mithilfe von ASP können Sie Daten aus Syslog-Nachrichten auf der Basis benutzerdefinierter Regeln analysieren.

Mit den Regeln weisen Sie ASP an, wie eine bestimmte Nachricht erkannt werden soll und wo in diesem nachrichtenspezifischen Ereignis sich Daten wie beispielsweise Signatur-IDs, IP-Adressen, Ports, Benutzernamen und Aktionen befinden.

Außerdem können Sie so optimal komplexe Protokollquellen wie Linux- und UNIX-Server sortieren. Für diese Funktionalität müssen Sie an die Linux- oder UNIX-Umgebung angepasste Regeln schreiben.



Außerdem sind Kenntnisse von regulären Ausdrücken erforderlich.

Wenn das System ein ASP-Protokoll empfängt, muss das Zeitformat mit dem in der ASP-Regel angegebenen Format übereinstimmen. Anderenfalls wird das Protokoll nicht verarbeitet. Sie können mehrere benutzerdefinierte Zeitformate hinzufügen, um die Wahrscheinlichkeit zu erhöhen, dass das Zeitformat für das Protokoll übereinstimmt (siehe *Hinzufügen von Zeitformaten zu ASP-Regeln*).

Wenn Sie über Rechte als **Richtlinienadministrator** verfügen, können Sie die Reihenfolge für die Ausführung der ASP-Regeln definieren. Mit diesen Regeln werden dann die Daten generiert, die Sie benötigen (siehe *Festlegen der Reihenfolge für ASP-Regeln und Filterregeln*).

Hinzufügen einer benutzerdefinierten ASP-Regel

Mit dem Editor für **Regel für erweiterten Syslog-Parser** können Sie Regeln zum Analysieren von ASP-Protokolldaten erstellen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** Folgendes aus: **Empfänger** | **Erweiterter Syslog-Parser**.

2 Wählen Sie **Neu** aus, und klicken Sie dann auf **Regel für erweiterten Syslog-Parser**.

3 Klicken Sie auf die einzelnen Registerkarten, und geben Sie die erforderlichen Informationen ein.

4 Klicken Sie auf **Fertig stellen**.

Festlegen der Reihenfolge für ASP-Regeln und Filterregeln

Wenn Sie über Rechte als **Richtlinienadministrator** verfügen, können Sie jetzt die Ausführungsreihenfolge für Filterregeln oder für ASP-Regeln festlegen. Mit dieser Option werden die Regeln in der Reihenfolge sortiert, mit der Sie die benötigten Daten auf die effizienteste Weise erhalten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ESM-Konsole auf das Symbol **Richtlinien-Editor**  .

2 Wählen Sie im Menü **Vorgänge** die Option **Reihenfolge für ASP-Regeln festlegen** oder **Reihenfolge für Filterregeln festlegen** aus. Wählen Sie dann im Feld **Datenquellentyp** eine Datenquelle aus.

Der linke Bereich wird mit den Regeln ausgefüllt, die zum Sortieren verfügbar sind. Die sortierten Regeln werden im rechten Bereich angezeigt.

3 Verschieben Sie auf der Registerkarte **Standardregeln** oder **Benutzerdefinierte Regeln** eine Regel aus dem linken in den rechten Bereich (mit Ziehen und Ablegen oder mithilfe der Pfeile) über oder unter **Regeln ohne Reihenfolge**.



Regeln ohne Reihenfolge entspricht den Regeln im linken Bereich, die in der Standardreihenfolge angeordnet sind.

4 Ändern Sie die Reihenfolge der Regeln mithilfe der Pfeile, und klicken Sie dann auf **OK**, um die Änderungen zu speichern.

Hinzufügen von Zeitformaten zu ASP-Regeln

Wenn das System ein Protokoll des erweiterten Syslog-Parsers (ASP) empfängt, muss das Zeitformat mit dem in der ASP-Regel angegebenen Format übereinstimmen.

Sie können mehrere benutzerdefinierte Zeitformate hinzufügen, um die Wahrscheinlichkeit zu erhöhen, dass das Zeitformat für das Protokoll mit einem der angegebenen Formate übereinstimmt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ESM-Konsole auf das Symbol **Richtlinien-Editor** .

2 Klicken Sie im Bereich **Regeltypen** auf **Empfänger** | **Erweiterter Syslog-Parser**.

3 Führen Sie nach dem Herunterladen der ASP-Regeln eine der folgenden Aktionen aus:

- Zum Bearbeiten einer vorhandenen Regel klicken Sie auf die Regel und dann auf **Bearbeiten** | **Ändern**.
- Zum Hinzufügen einer neuen Regel klicken Sie auf **Neu** | **Regel für erweiterten Syslog-Parser**, und füllen Sie dann die Registerkarten **Allgemein**, **Analysieren** und **Feldzuweisung** aus.

4 Klicken Sie auf die Registerkarte **Zuordnung** und dann auf das Pluszeichen über der Tabelle **Zeitformat**.

5 Klicken Sie in das Feld **Format**, und wählen Sie dann das Zeitformat aus.

6 Wählen Sie die Uhrzeitfelder aus, für die Sie das Format verwenden möchten.

Mit **Erstes Mal** und **Letztes Mal** wird angegeben, wann das Ereignis zum ersten bzw. zum letzten Mal generiert wurde. Außerdem werden alle Uhrzeitfelder vom Typ **Benutzerdefinierter Typ** aufgeführt, die Sie zu ESM hinzugefügt haben (siehe *Benutzerdefinierte Typfilter*).

7 Klicken Sie auf **OK**, und geben Sie dann die verbleibenden Informationen auf der Registerkarte **Zuordnung** ein.

Datenquellenregeln

Die Liste der Datenquellenregeln enthält vordefinierte und automatisch erlernte Regeln.

Der Empfänger erlernt automatisch Datenquellenregeln bei der Verarbeitung der Informationen, die von den ihm zugeordneten Datenquellen an ihn gesendet werden.

Die Option **Datenquelle** im Bereich **Regeltypen** ist nur sichtbar, wenn in der Systemnavigationsstruktur eine Richtlinie, eine Datenquelle, ein **Erweiterter Syslog-Parser** oder ein Empfänger ausgewählt ist. Der Beschreibungsbereich unten auf der Seite enthält detaillierte Informationen zur ausgewählten Regel. Alle Regeln verfügen über eine Schweregradeinstellung, mit der die einer Regel zugeordnete Priorität vorgegeben wird. Die Priorität wirkt sich darauf aus, wie die für die jeweiligen Regeln generierten Warnungen zu Berichterstellungszwecken angezeigt werden.

Für Datenquellenregeln ist eine Standardaktion definiert. Diese Aktion wird vom Empfänger dem der Regel zugeordneten Ereignisuntertyp zugewiesen. Sie können die Aktion ändern (siehe *Festlegen von Aktionen für Datenquellenregeln*).

Festlegen von Aktionen für Datenquellenregeln

Für Datenquellenregeln ist eine Standardaktion definiert. Diese Aktion wird vom Empfänger dem der Regel zugeordneten Ereignisuntertyp zugewiesen. Sie können die Aktion ändern.

Sie können den Wert des Ereignisuntertyps über eine Datenquellenregel festlegen. Dies bedeutet, dass Sie Regelaktionen für Dashboards, Berichte, Analyseregeln oder Alarme mit verschiedenen Werten festlegen können, beispielsweise mit dem Ergebnis einer selektiven Zugriffsregel (Zulassen/Verweigern).

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ESM-Konsole auf das Symbol **Richtlinien-Editor**  , und wählen Sie dann **Empfänger** | **Datenquelle** im Bereich **Regeltypen** aus.

2 Klicken Sie in die Spalte **Untertyp** für die zu ändernde Regel, und wählen Sie dann die neue Aktion aus.

- Wählen Sie **Aktivieren** aus, um den Ereignisuntertyp mit der Standardaktion **Warnung** auszufüllen.
- Wählen Sie **Deaktivieren** aus, wenn Sie für die entsprechende Regel keine Ereignisse erfassen möchten.
- Wählen Sie beliebige weitere Aktionen aus, um den Ereignisuntertyp mit der jeweiligen Aktion auszufüllen.

Verwalten automatisch erlernter Datenquellenregeln

Zeigen Sie eine Liste aller automatisch erlernten Datenquellenregeln an, und bearbeiten oder löschen Sie sie.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** Folgendes aus: **Empfänger** | **Datenquelle**.

2 Klicken Sie unten im Bereich **Filter/Kennzeichnung** auf die Leiste **Erweitert**.

3 Wählen Sie in der Dropdown-Liste **Herkunft** die Option **benutzerdefiniert** aus, und klicken Sie dann auf das Symbol **Abfrage ausführen**  .

Alle automatisch erlernten Datenquellenregeln werden im Anzeigebereich aufgeführt.

4 Wählen Sie die zu bearbeitende oder zu löschende Regel aus, klicken Sie auf **Bearbeiten**, und wählen Sie dann **Ändern** oder **Automatisch erlernte Regeln löschen** aus.

- Wenn Sie **Ändern** ausgewählt haben, ändern Sie den Namen, die Beschreibung oder die normalisierte ID, und klicken Sie dann auf **OK**.
- Wenn Sie **Automatisch erlernte Regeln löschen** ausgewählt haben, wählen Sie die richtige Option aus, und klicken Sie dann auf **OK**.

Windows-Ereignisregeln

Windows-Ereignisregeln werden verwendet, um Ereignisse im Zusammenhang mit Windows zu generieren.

Hierbei handelt es sich um Datenquellenregeln für Windows-Ereignisse, die vom Typ der Datenquellenregel getrennt sind, da sie allgemein verwendet werden. Alle Regeln dieses Typs werden von McAfee definiert. Sie können die Regeln nicht hinzufügen, ändern oder löschen. Sie können jedoch ihre Eigenschaftseinstellungen ändern.

ADM-Regeln

McAfee ADM besteht aus einer Reihe von Netzwerk-Appliances, die auf dem DPI-Modul (Deep Packet Inspection) von ICE beruhen.

Beim ICE-Modul handelt es sich um eine Software-Bibliothek und Sammlung von Plug-In-Modulen für Protokolle und Inhalte, mit denen Inhalte aus unbearbeitetem Netzwerkverkehr in Echtzeit identifiziert und extrahiert werden können. Inhalte auf Anwendungsebene können vollständig erneut zusammengestellt und decodiert werden. Dabei werden Streams aus kryptischen Netzwerkpaketen in Inhalte umgewandelt, die so leicht lesbar sind wie der Inhalt einer lokalen Datei.

Sie können mit dem ICE-Modul automatisch Protokolle und Inhaltstypen identifizieren und sind dabei nicht auf feste TCP-Port-Nummern oder Dateierweiterungen angewiesen. Die Analyse und Decodierung über das ICE-Modul erfolgt ohne Zuhilfenahme von Signaturen. Stattdessen werden durch die einzelnen Module für jedes Protokoll bzw. jeden Inhaltstyp vollständige Parser implementiert. Dadurch ergibt sich eine äußerst genaue Identifizierung und Decodierung der Inhalte, die auch dann identifiziert und extrahiert werden können, wenn sie komprimiert oder anderweitig codiert sind und daher im Netzwerk nicht als Klartext übertragen werden.

Aufgrund dieser sehr genauen Identifizierung und Decodierung bietet das ICE-Modul besonders tiefe Einblicke in den Netzwerkverkehr. Beispielsweise könnte das ICE-Modul einen PDF-Dokument-Stream, der das Netzwerk in einer ZIP-Datei durchquert hat, als BASE-64-codierten Anhang einer SMTP-E-Mail von einem SOCKS-Proxyserver empfangen.

Durch diese Erkennung von Anwendungen und Dokumenten ergibt sich mithilfe von ADM ein Sicherheitskontext von unschätzbarem Wert. Sie können Bedrohungen entdecken, die mit herkömmlichen IDS-Systemen oder Nitro IPS nicht entdeckt werden können, beispielsweise:

- Verlust vertraulicher Informationen und Dokumente oder Verletzungen von Kommunikationsrichtlinien
- Nicht autorisierter Datenverkehr durch Anwendungen (Beispiel: Wer verwendet Gnutella?)
- Anwendungen, die auf unerwartete Weise verwendet werden (beispielsweise HTTPS an einem Nicht-Standard-Port)
- Potenziell böswillige Dokumente (beispielsweise ein Dokument, das nicht mit seiner Erweiterung übereinstimmt)
- Neue Generation von Exploits (beispielsweise ein PDF-Dokument mit einer eingebetteten ausführbaren Datei)

Darüber hinaus werden mit ADM böswillige Verkehrsmuster entdeckt, indem Anomalien in Anwendungs- und Transportprotokollen entdeckt werden (beispielsweise eine falsch formatierte RPC-Verbindung oder der TCP-Ziel-Port 0).

Unterstützte Anwendungen und Protokolle

Mit ADM können Anomalien in mehr als 500 unterstützten Anwendungen und Protokollen überwacht, decodiert und erkannt werden. Die folgende Liste enthält einige Beispiele:

- Low-Level-Netzwerkprotokolle: TCP/IP, UDP, RTP, RPC, SOCKS, DNS und andere
- E-Mail: MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- Chat: MSN, AIM/Oscar, Yahoo, Jabber, IRC
- Web-Mail: AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook und MySpace-E-Mail
- P2P: Gnutella, BitTorrent
- Shell: SSH (nur Entdeckung), Telnet

- Instant Messaging: AOL, ICQ, Jabber, MSN, SIP und Yahoo
- Dateiübertragungsprotokolle: FTP, HTTP, SMB und SSL
- Komprimierungs- und Extrahierungsprotokolle: BASE64, GZIP, MIME, TAR, ZIP und andere
- Archivdateien: RAR-Archive, ZIP, BZIP, GZIP, Binhex und UU-codierte Archive
- Installationspakete: Linux-Pakete, InstallShield-CAB-Dateien, Microsoft-CAB-Dateien
- Bilddateien: GIF, JPEG, PNG, TIFF, AutoCAD, Photoshop, Bitmaps, Visio, Digital RAW und Windows-Symbole
- Audiodateien: WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio, SHOUTCast und weitere
- Videodateien: AVI, Flash, QuickTime, Real Media, MPEG-4, Vivo, Digital Video (DV), Motion JPEG und weitere
- Sonstige Anwendungen und Dateien: Datenbanken, Tabellen, Faxe, Web-Anwendungen, Schriftarten, ausführbare Dateien, Microsoft Office-Anwendungen, Spiele und sogar Tools für die Software-Entwicklung
- Sonstige Protokolle: Netzwerkdrucker, Shell-Zugriff, VoIP und Peer-to-Peer

Wichtige Konzepte

Um die Funktionsweise von ADM zu verstehen, müssen Sie die folgenden Konzepte kennen:

- **Objekt**: Ein Objekt ist ein einzelnes Inhaltselement. Eine E-Mail ist ein Objekt, aber auch ein Objekt-Container, da sie einen Textteil (oder zwei Textteile) und Anhänge enthält. Eine HTML-Seite ist ein Objekt, das weitere Objekte enthalten kann, beispielsweise Bilder. ZIP-Dateien ebenso wie die darin enthaltenen Dateien sind Objekte. Der Container wird von ADM entpackt, und jedes enthaltene Objekt wird als eigenes Objekt behandelt.
- **Transaktion**: Eine Transaktion ist ein Wrapper um die Übertragung eines Objekts (Inhalts). Eine Transaktion enthält mindestens ein Objekt. Wenn dieses Objekt jedoch ein Container ist (beispielsweise eine ZIP-Datei), kann eine einzelne Transaktion mehrere Objekte enthalten.
- **Fluss**: Ein Fluss ist die TCP- oder UDP-Netzwerkverbindung. Ein Fluss kann viele Transaktionen enthalten.

DEM-Regeln

Die Stärke von McAfee DEM ist die Art der Aufzeichnung und Normalisierung der Informationen in Netzwerkpaketen.

Mit DEM können Sie außerdem komplexe Regeln erstellen und dabei logische und reguläre Ausdrücke für den Mustervergleich verwenden. So können Sie Datenbank- oder Anwendungsnachrichten praktisch ohne False-Positives überwachen. Die normalisierten Daten (Messgrößen) unterscheiden sich je nach Anwendung, da manche Anwendungsprotokolle und -nachrichten umfangreicher sind als andere. Filterausdrücke müssen sorgfältig erstellt werden. Dabei müssen Sie nicht nur auf die Syntax achten, sondern auch sicherstellen, dass die Messgröße für die Anwendung unterstützt wird.

Im Lieferumfang des DEM-Geräts ist ein Standardregelsatz enthalten. Mit Standard-Compliance-Regeln können Sie wichtige Datenbankereignisse überwachen, beispielsweise An- und Abmeldungen, DBA-typische Aktivitäten wie DDL-Änderungen, verdächtige Aktivitäten und Datenbankangriffe, bei denen normalerweise Compliance-Anforderungen erfüllt sein müssen. Sie können die einzelnen Standardregeln aktivieren oder deaktivieren und die Werte der vom Benutzer definierbaren Parameter für die einzelnen Regeln festlegen.

Die folgenden DEM-Regeltypen stehen zur Verfügung: Datenbank, Datenzugriff, Erkennung und Transaktionsüberwachung

Regeltypen	Beschreibung
Datenbank	Der DEM-Standardregelsatz enthält Regeln für die einzelnen unterstützten Datenbanktypen sowie für allgemeine Vorschriften wie SOX, PCI, HIPAA und FISMA. Sie können die einzelnen Standardregeln aktivieren oder deaktivieren und die Werte der vom Benutzer definierbaren Parameter für die einzelnen Regeln festlegen. Neben den im Lieferumfang des DEM-Geräts enthaltenen Regeln können Sie komplexe Regeln mit logischen und regulären Ausdrücken erstellen. So können Sie Datenbank- oder Anwendungsnachrichten praktisch ohne False-Positives überwachen. Da manche Anwendungsprotokolle und -nachrichten umfangreicher sind als andere, unterscheiden sich die normalisierten Daten (Messgrößen) je nach Anwendung. Sie können beliebig komplexe Regeln erstellen und dabei Operatoren für logische und reguläre Ausdrücke verwenden. Ein Regelausdruck kann auf eine oder mehrere für die Anwendung verfügbare Messgrößen angewendet werden.
Datenzugriff	Mithilfe von DEM-Datenzugriffsregeln können Sie unbekannte Zugriffspfade in die Datenbank verfolgen und Warnungen in Echtzeit senden. Wenn Sie die richtigen Datenzugriffsregeln erstellen, können Sie allgemeine Verletzungen in Datenbankumgebungen leicht verfolgen, beispielsweise Anwendungsentwickler, die mit Anmelde-IDs für Anwendungen auf Produktionssysteme zugreifen.

Regeltypen	Beschreibung
Erkennung	Mit den DEM-Regeln für die Datenbankerkennung erhalten Sie eine Ausnahmeliste von Datenbank-Servern, die von ESM unterstützt werden und sich im Netzwerk befinden, aber nicht überwacht werden. Auf diese Weise kann ein Sicherheitsadministrator zur Umgebung hinzugefügte neue Datenbank-Server erkennen sowie verbotene Listener-Ports, die geöffnet wurden, um auf Daten aus Datenbanken zuzugreifen. Bei den Erkennungsregeln (**Richtlinien-Editor** | **DEM-Regeltyp** | **Erkennung**) handelt es sich um direkt nach der Installation verfügbare Regeln, die nicht hinzugefügt oder bearbeitet werden können. Wenn die Option Erkennung auf der Seite Datenbank-Server aktiviert ist (**DEM-Eigenschaften** | **Datenbank-Server** | **Aktivieren**), werden diese Regeln vom System verwendet, um nach Datenbank-Servern im Netzwerk zu suchen, die nicht in der Systemnavigationsstruktur unter dem DEM-Gerät aufgeführt sind.
Transaktionsüberwachung	Mit Transaktionsüberwachungsregeln können Sie Datenbanktransaktionen verfolgen und Änderungen automatisch abgleichen. Beispielsweise können Sie die zeitraubende Überwachung von Datenbankänderungen und den Abgleich mit autorisierten Arbeitsaufträgen in einem vorhandenen Ticket-System vollständig automatisieren. Die Verwendung dieser Funktion lässt sich am besten anhand eines Beispiels veranschaulichen: Der DBA führt im Rahmen des Verfahrens die gespeicherte Prozedur für das Start-Tag (in diesem Beispiel spChangeControlStart) in der Datenbank aus, in der die Arbeit ausgeführt werden soll, bevor die autorisierte Arbeit tatsächlich beginnt. Mit der DEM-Funktion **Transaktionsüberwachung** kann der DBA bis zu drei optionale Zeichenfolgenparameter als Argument in der richtigen Reihenfolge in das Tag einschließen: **1** ID **2** Name oder DBA-Initialen **3** Kommentar Beispiel: `spChangeControlStart '12345', 'mshakir', 'reindexing app'` Wenn vom DEM-Gerät die Ausführung der gespeicherten Prozedur spChangeControlStart beobachtet wird, werden die Transaktion sowie die Parameter (ID, Name, Kommentar) als spezielle Informationen protokolliert. Nach Abschluss der Arbeit führt der DBA die gespeicherte Prozedur für das End-Tag (spChangeControlEnd) aus und schließt optional einen ID-Parameter ein, der mit der ID im Start-Tag identisch sein muss. Wenn vom DEM-Gerät das End-Tag (und die ID) beobachtet wird, können alle Aktivitäten zwischen dem Start-Tag (mit der gleichen ID) und dem End-Tag als spezielle Transaktion zugeordnet werden. Sie können jetzt Berichte nach Transaktionen erstellen und nach der ID suchen, bei der es sich in diesem Beispiel für den Abgleich eines Arbeitsauftrags um die Change Control-Nummer handeln kann. Außerdem können Sie mit der Transaktionsüberwachung Start und Ende einer Handelsausführung oder sogar Begin- und Commit-Anweisungen protokollieren, um Berichte nach Transaktionen anstelle von Abfragen zu erstellen.

Messgrößenreferenzen für DEM-Regeln

Nachfolgend finden Sie eine Liste mit Messgrößenreferenzen für die DEM-Regelausdrücke, die beim Hinzufügen einer DEM-Regel auf der Seite **Ausdruckskomponente** zur Verfügung stehen.

Name	Beschreibung	Datenbanktypen
Anwendungsname	Der Name zur Identifizierung des Datenbanktyps, für den die Regel gilt.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PIServer, InterSystems Caché
Startzeit	Zeitstempel für die Startzeit der Abfrage	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Versatz für Startzeit	Zeichnet den Versatz der Server-Uhrzeit auf.	MSSQL, Oracle, DB2, Sybase, MySQL, PostgreSQL, Teradata, PIServer, InterSystems Caché
Client-IP	IP-Adresse des Clients	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Client-Name	Name des Client-Computers	MSSQL, Oracle, DB2, Sybase, Informix, PIServer, InterSystems Caché
Client-PID	Die Prozess-ID, die dem Client-Prozess vom Betriebssystem zugewiesen wurde.	MSSQL, DB2, Sybase, MySQL
Client-Port	Port-Nummer der Socket-Verbindung des Clients	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Befehlsname	Name des MySQL-Befehls	MSSQL, Oracle, DB2, Sybase, Informix
Befehlstyp	Typ des MySQL-Befehls: DDL, DML, Anzeigen oder Replizierung	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Eingehende Daten	Gesamtanzahl der Bytes im eingehenden Abfragepaket	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Ausgehende Daten	Gesamtanzahl der Bytes in den ausgehenden Ergebnispaketen	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché

Name	Beschreibung	Datenbanktypen
Datenbankname	Name der Datenbank, auf die zugegriffen wird.	MSSQL, DB2, Sybase, MySQL, Informix, PostgreSQL, PIServer, InterSystems Caché
Endzeit	Abschlusszeitstempel für das Ende der Abfrage	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Fehlermeldung	Enthält den Nachrichtentext, der den Variablen SQLCODE und SQLSTATE in der SQLCA-Datenstruktur (SQL Communication Area) zugeordnet ist und Informationen zum Erfolg oder Fehlschlagen der angeforderten SQL-Anweisungen enthält.	DB2, Informix
Nachrichtennummer	Eine eindeutige Nachrichtennummer, die jedem Fehler vom Datenbank-Server zugewiesen wird.	MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Caché
Nachrichtenschweregrad	Zahl für den Schweregrad zwischen 10 und 24, die Typ und Schweregrad des Problems angibt.	MSSQL, Sybase, Informix
Nachrichtentext	Vollständiger Text der Nachricht	MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Caché
Netzwerkzeit	Zeitbedarf für das Senden des Ergebnissatzes zurück an den Client (Antwortzeit – Antwortzeit des Servers)	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
NT-Client-Name	Name des Windows-Computers, über den sich der Benutzer angemeldet hat.	MSSQL
NT-Domänenname	Name der Windows-Domäne, aus der sich der Benutzer angemeldet hat.	MSSQL
NT-Benutzername	Anmeldename des Windows-Benutzers	MSSQL
Objektname		MSSQL, Oracle, DB2, Sybase, MySQL, Informix
OSS-Benutzername		Oracle
Paketname	Ein Paket enthält Steuerungsstrukturen, die zum Ausführen von SQL-Anweisungen verwendet werden. Pakete werden bei der Programmvorbereitung erzeugt und mit dem DB2-Unterbefehl BIND PACKAGE erstellt.	DB2
Eingehende Pakete	Anzahl der Pakete, aus denen die Abfrage besteht.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché

Name	Beschreibung	Datenbanktypen
Ausgehende Pakete	Anzahl der Pakete, aus denen der zurückgegebene Ergebnissatz besteht.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Kennwort		MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, InterSystems Caché
Kennwortlänge		MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, InterSystems Caché
Größe des Abfrageblocks	Ein Abfrageblock ist die Basiseinheit für die Übertragung von Daten in Abfragen und Ergebnissätzen. Durch Festlegen der Größe des Abfrageblocks kann der Anfrager, für den möglicherweise Ressourceneinschränkungen gelten, die Menge der jeweils zurückgegebenen Daten steuern.	DB2, Informix
Beendigungsstatus der Abfrage	Beendigungsstatus einer Abfrage	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Caché
Abfragenummer	Eine eindeutige Nummer, die jeder Abfrage vom AuditProbe-Überwachungs-Agenten zugewiesen wird. Die erste Abfrage erhält die Nummer 0, und die folgenden werden jeweils um 1 erhöht.	MSSQL, Oracle, DB2, Sybase, MySQL, PostgreSQL, Teradata, PIServer, InterSystems Caché
Abfragetext	Die tatsächliche vom Client gesendete SQL-Abfrage.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Abfragetyp	Eine Ganzzahl, die verschiedenen Abfragetypen zugewiesen wird.	MSSQL, Oracle, Sybase
Tatsächlicher Benutzername	Anmeldename des Client-Benutzers	
Antwortinhalt		MSSQL, Oracle, DB2, Sybase, MySQL, Informix
Antwortzeit	End-to-End-Antwortzeit der Abfrage (Antwortzeit des Servers + Netzwerkzeit)	MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Caché
Zurückgegebene Zeilen	Anzahl der Zeilen im zurückgegebenen Ergebnissatz	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché

Name	Beschreibung	Datenbanktypen
Sicherheitskennzeichnung	Messgröße für die Sicherheitskennzeichnung, deren Wert auf 1 (VERTRAUENSWÜRDIG) oder 2 (NICHT VERTRAUENSWÜRDIG) festgelegt ist, wenn vom Administrator festgelegte Kriterien für die Zugriffsrichtliniendatei erfüllt sind. Der Wert 3 bedeutet, dass die Kriterien für die Richtliniendatei nicht erfüllt sind. Der Wert 0 bedeutet, dass die Sicherheitsüberwachung nicht aktiviert ist.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems
Sicherheitsmechanismus	Der Sicherheitsmechanismus, mit dem die Identität des Benutzers überprüft wird (beispielsweise Benutzer-ID und Kennwort).	DB2
Server-IP	IP-Adresse des Datenbank-Server-Hosts	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Caché
Server-Name	Dies ist der Name des Servers. Der Hostname wird standardmäßig als Server-Name zugewiesen.	MSSQL, Oracle, DB2, Sybase, Informix, PIServer, InterSystems Caché
Server-Port	Port-Nummer des Servers	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Caché
Antwortzeit des Servers	Anfängliche Antwort vom Datenbank-Server auf die Client-Abfrage	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
Schweregrad-Code		DB2
SID	Oracle-System-ID	Oracle, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché
SPID	Die jeder eindeutigen Verbindung bzw. Sitzung zugewiesene Prozess-ID für das Datenbanksystem.	MSSQL, Sybase

Name	Beschreibung	Datenbanktypen
SQL-Code	Bei jeder Ausführung einer SQL-Anweisung empfängt der Client einen SQL-Code (SQLCODE). Dabei handelt es sich um einen Rückgabe-Code, der zusätzliche DB2-spezifische Informationen zu einem SQL-Fehler oder einer SQL-Warnung enthält: • SQLCODE EQ 0 bedeutet, dass die Anweisung erfolgreich ausgeführt wurde. • SQLCODE GT 0 bedeutet, dass die Anweisung mit einer Warnung erfolgreich ausgeführt wurde. • SQLCODE LT 0 bedeutet, dass die Anweisung nicht erfolgreich ausgeführt wurde. • SQLCODE EQ 100 bedeutet, dass keine Daten gefunden wurden. Die Bedeutung von SQL-Codes außer 0 und 100 hängt vom jeweiligen Produkt mit SQL-Implementierung ab.	
SQL-Befehl	Typ des SQL-Befehls	
SQL-Status	DB2 SQLSTATE ist ein zusätzlicher Rückgabe-Code, durch den Anwendungsprogramme allgemeine Rückgabe-Codes für allgemeine Fehlerbedingungen erhalten, die in den relationalen Datenbanksystemen von IBM auftreten.	DB2
Benutzername	Anmeldename des Datenbankbenutzers	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Caché

Korrelationsregeln

Der Hauptzweck des Korrelationsmoduls besteht darin, vom ESM-Gerät fließende Daten zu analysieren, relevante Muster innerhalb des Datenflusses zu entdecken, Warnungen zu generieren, die diese Muster darstellen, und die Warnungen in die Warnungsdatenbank des Empfängers einzufügen. Das Korrelationsmodul wird beim Konfigurieren einer Korrelationsdatenquelle aktiviert.

Innerhalb des Korrelationsmoduls führt ein relevantes Muster dazu, dass Daten von einer Korrelationsregel interpretiert werden. Eine Korrelationsregel ist ein vollständig von einer Firewall-Regel oder Standardregel getrenntes eindeutiges Element mit einem Attribut, das sein Verhalten festlegt. Jeder Empfänger erhält einen Satz von Korrelationsregeln von einem ESM-Gerät (bereitgestellter Korrelationsregelsatz), der aus null oder mehr Korrelationsregeln besteht, für die benutzerdefinierte Parameterwerte festgelegt sind. Neben Firewall-Regelsätzen und Standardregelsätzen ist in jedem ESM-Gerät ein Satz von Basiskorrelationsregeln enthalten. Aktualisierungen für diesen Regelsatz werden vom Regelaktualisierungs-Server auf ESM-Geräten bereitgestellt.



Die Regeln auf dem Regelaktualisierungs-Server enthalten Standardwerte. Wenn Sie den Basisregelsatz für das Korrelationsmodul aktualisieren, müssen Sie diese Standardwerte an Ihr Netzwerk anpassen. Wenn Sie die Regeln bereitstellen, ohne die Standardwerte zu ändern, werden möglicherweise False-Positives oder False-Negatives generiert.

Sie können ähnlich wie beim Konfigurieren von Syslog oder OPSEC nur eine Korrelationsdatenquelle pro Empfänger konfigurieren. Wenn Sie die Korrelationsdatenquelle konfiguriert haben, können Sie den Satz von Basiskorrelationsregeln bearbeiten, um den bereitgestellten Korrelationsregelsatz mit dem **Editor für Korrelationsregeln** zu erstellen. Sie können die einzelnen Korrelationsregeln aktivieren oder deaktivieren und die Werte der vom Benutzer definierbaren Parameter für die einzelnen Regeln festlegen.

Neben dem Aktivieren oder Deaktivieren der Korrelationsregeln können Sie mit dem **Editor für Korrelationsregeln** benutzerdefinierte Regeln und Korrelationskomponenten erstellen, die zu benutzerdefinierten Korrelationsregeln hinzugefügt werden können.

Anzeigen von Details zu Korrelationsregeln

Für Korrelationsregeln werden jetzt Details zu der Ursache angezeigt, durch die die Regel ausgelöst wurde. Anhand dieser Informationen können Sie die Anzahl der False-Positives verringern.

Details werden immer zum Zeitpunkt der Anfrage auf der Benutzeroberfläche gesammelt. Für Regeln, bei denen dynamische Watchlists oder andere häufig geänderte Werte verwendet werden, können Sie festlegen, dass die Details unmittelbar nach der Auslösung abgerufen werden. Dadurch verringert sich die Wahrscheinlichkeit, dass Details nicht mehr verfügbar sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Legen Sie für jede Regel fest, dass die Details sofort angezeigt werden:

   a Klicken Sie in der ESM-Konsole auf das Schnellstartsymbol für **Korrelation** .

   Daraufhin wird der **Richtlinien-Editor** geöffnet, in dem der Regeltyp **Korrelation** ausgewählt ist.

   b Klicken Sie in die Spalte **Details** für die Regel, und wählen Sie die Option **An** aus.

   Sie können mehrere Regeln gleichzeitig auswählen.

2 Zeigen Sie die Details an:

   a Klicken Sie in der Systemnavigationsstruktur unter dem ACE-Gerät auf **Regelkorrelation**.

   b Wählen Sie in der Liste der Ansichten die Optionen **Ereignisansichten** | **Ereignisanalyse**aus, und klicken Sie dann auf das anzuzeigende Ereignis.

   c Klicken Sie auf die Registerkarte **Korrelationsdetails**, um die Details anzuzeigen.

Hinzufügen benutzerdefinierter ADM-Regeln, Datenbankregeln oder Korrelationsregeln

Sie können nicht nur die vordefinierten ADM-Regeln, Datenbankregeln oder Korrelationsregeln verwenden, sondern auch komplexe Regeln mit logischen und regulären Ausdrücken erstellen. Die Editoren, die Sie zum Hinzufügen dieser verschiedenen Regeltypen verwenden, sind sich sehr ähnlich und werden daher in den gleichen Abschnitten beschrieben.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** die Option **ADM**, **DEM** | **Database**oder **Korrelation** aus.

2 Klicken Sie auf **Neu**, und wählen Sie dann den Regeltyp aus, den Sie hinzufügen möchten.

3 Geben Sie die erforderlichen Informationen ein. Ziehen Sie dann logische Elemente und Ausdruckskomponenten aus der Symbolleiste in den Bereich **Ausdruckslogik**, und legen Sie sie dort ab, um die Logik der Regel zu erstellen.

4 Klicken Sie auf **OK**.

Aufgaben

- *Hinzufügen von Parametern zu einer Korrelationsregel oder -komponente* auf Seite 355
  Durch die Parameter einer Korrelationsregel oder -komponente wird das Verhalten der Regel oder Komponente bei der Ausführung gesteuert. Parameter sind nicht erforderlich.
- *Hinzufügen oder Bearbeiten einer Datenzugriffsregel* auf Seite 358
  Mithilfe von DEM-Datenzugriffsrichtlinien können Sie unbekannte Zugriffspfade in die Datenbank verfolgen und Ereignisse in Echtzeit senden.
- *Hinzufügen oder Bearbeiten einer Transaktionsüberwachungsregel* auf Seite 358
  Mit Transaktionsüberwachungsregeln können Sie Datenbanktransaktionen verfolgen und Änderungen automatisch abgleichen sowie Start und Ende einer Handelsausführung oder Begin- und Commit-Anweisungen protokollieren, um Berichte nach Transaktionen anstelle von Abfragen zu erstellen.
- *Verwalten benutzerdefinierter ADM-Regeln, DEM-Regeln oder Korrelationsregeln* auf Seite 358
  Kopieren Sie eine vordefinierte Regel, und verwenden Sie diese als Vorlage für eine benutzerdefinierte Regel. Beim Hinzufügen einer benutzerdefinierten Regel können Sie die Einstellungen bearbeiten, kopieren und einfügen, um die Regel als Vorlage für eine neue benutzerdefinierte Regel zu verwenden, oder die Einstellungen löschen.
- *Einrichten einer Regel und eines Berichts für Datenbank-Audit-Listen* auf Seite 359
  Im Bericht **Audit-Listen für berechtigte Benutzer** können Sie die Audit-Liste für Änderungen an der Datenbank anzeigen oder den Zugriff auf eine Datenbank oder Tabelle verfolgen, der einem bestimmten Datenbankereignis zugeordnet war.

Logische Elemente

Wenn Sie eine ADM-Regel, Datenbankregel und Korrelationsregel oder Korrelationskomponente hinzufügen, müssen Sie die Kernfunktionalität der Regel erstellen, indem Sie die logischen Elemente in den Bereich **Ausdruckslogik** oder **Korrelationslogik** ziehen. Die logischen Elemente bilden das Gerüst für die Regel.

Element		Beschreibung
	AND	Funktioniert wie ein logischer Operator in einer Computersprache. Alle unter diesem logischen Element gruppierten Elemente müssen wahr sein, damit die Bedingung wahr ist. Verwenden Sie diese Option, wenn alle Bedingungen dieses logischen Elements erfüllt sein müssen, damit eine Regel ausgelöst wird.
	OR	Funktioniert wie ein logischer Operator in einer Computersprache. Nur eine unter diesem Element gruppierte Bedingung muss wahr sein, damit diese Bedingung wahr ist. Verwenden Sie dieses Element, wenn nur eine Bedingung erfüllt sein muss, damit die Regel ausgelöst wird.
	SET	Für Korrelationsregeln oder Komponenten können Sie mit diesem Element mehrere Bedingungen definieren und die Anzahl der Bedingungen auswählen, die wahr sein müssen, damit die Regel ausgelöst wird. Wenn der Satz beispielsweise drei Bedingungen enthält, die erfüllt sein müssen, damit die Regel ausgelöst wird, lautet der Satz "2 von 3".

Jedes dieser Elemente hat ein Menü mit mindestens zwei der folgenden Optionen:

- **bearbeiten**: Sie können die Standardeinstellungen bearbeiten (siehe *Bearbeiten der Standardeinstellungen für logische Elemente*).
- **logisches Element entfernen**: Sie können das ausgewählte logische Element löschen. Wenn untergeordnete Elemente vorhanden sind, werden diese nicht gelöscht und in der Hierarchie nach oben verschoben.

  Dies gilt nicht für das Stammelement (das erste Element in der Hierarchie). Wenn Sie das Stammelement entfernen, werden alle untergeordneten Elemente ebenfalls entfernt.

- **logisches Element und alle untergeordneten Elemente entfernen**: Sie können das ausgewählte Element und alle untergeordneten Elemente aus der Hierarchie löschen.

Beim Einrichten der Logik für die Regel müssen Sie Komponenten hinzufügen, um die Bedingungen für die Regel zu definieren. Für Korrelationsregeln können Sie außerdem Parameter hinzufügen, um das Verhalten der Regel oder Komponente bei der Ausführung zu steuern.

Bearbeiten logischer Elemente

Die logischen Elemente AND, OR und SET haben Standardeinstellungen. Diese können Sie auf der Seite **Logisches Element bearbeiten** ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Ziehen Sie im Regel-Editor ein logisches Element in den Bereich **Ausdruckslogik** oder **Korrelationslogik**, und legen Sie es dort ab.

2 Klicken Sie auf das Symbol **Menü** für das zu bearbeitende Element und dann auf **Bearbeiten**.

3 Ändern Sie die Einstellungen, und klicken Sie dann auf **OK**.

Hinzufügen von Parametern zu einer Korrelationsregel oder -komponente

Durch die Parameter einer Korrelationsregel oder -komponente wird das Verhalten der Regel oder Komponente bei der Ausführung gesteuert. Parameter sind nicht erforderlich.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf der Seite **Korrelationsregel** oder **Korrelationskomponente** auf **Parameter**.

2 Klicken Sie auf **Hinzufügen**, und geben Sie dann einen Namen für den Parameter ein.

3 Wählen Sie den Typ des gewünschten Parameters aus, und wählen Sie dann die Werte aus, oder heben Sie die Auswahl von Werten auf.

Sie können nicht gleichzeitig Werte für **Liste** und **Bereich** verwenden. Ein Listenwert kann keinen Bereich enthalten (1 – 6 8, 10, 13). Die richtige Schreibweise hierfür lautet 1, 2, 3, 4, 5, 6, 8, 10, 13.

4 Zum Auswählen des Standardwerts für den Parameter klicken Sie auf das Symbol **Standardwert-Editor** .

5 Wenn der Parameter nicht extern sichtbar sein soll, heben Sie die Auswahl von **Extern sichtbar** auf. Der Parameter ist für den Bereich der Regel lokal.

6 Geben Sie eine Beschreibung für den Parameter ein, die auf der Seite **Regelparameter** im Textfeld **Beschreibung** angezeigt wird, wenn Sie den Parameter hervorheben.

7 Klicken Sie auf **OK** und dann auf **Schließen**.

Beispiel für eine benutzerdefinierte Korrelationsregel oder -komponente

Hinzufügen einer Korrelationsregel oder -komponente

Mit der in diesem Beispiel hinzugefügten Regel wird eine Warnung generiert, wenn von ESM innerhalb von zehn Minuten fünf nicht erfolgreiche Anmeldeversuche von einer einzigen Quelle auf einem Windows-System entdeckt werden, auf die eine erfolgreiche Anmeldung folgt.

1 Klicken Sie im **Richtlinien-Editor** im Bereich **Regeltypen** auf **Korrelation**.

2 Klicken Sie auf **Neu**, und wählen Sie dann **Korrelationsregel** aus.

3 Geben Sie einen aussagekräftigen Namen ein, und wählen Sie dann die Schweregradeinstellung aus.



Da ein durch diese Regel generiertes Ereignis ein Hinweis darauf sein kann, dass eine nicht autorisierte Person auf das System zugegriffen hat, ist 80 eine geeignete Einstellung für den Schweregrad.

4 Wählen Sie die Normalisierungs-ID aus: **Authentifizierung** oder **Authentication | Anmeldung**. Ziehen Sie dann das logische Element **AND** an die gewünschte Stelle, und legen Sie es ab.



Wählen Sie **AND** aus, da zwei Aktionstypen auftreten müssen (zuerst Anmeldeversuche, dann eine erfolgreiche Anmeldung).

5 Klicken Sie auf das Symbol **Menü**  , und wählen Sie dann **Bearbeiten** aus.

6 Wählen Sie **Sequenz** aus, um anzugeben, dass die Aktionen (zuerst fünf nicht erfolgreiche Anmeldeversuche und dann eine erfolgreiche Anmeldung) der Reihe nach auftreten müssen. Legen Sie dann fest, wie oft diese Sequenz auftreten muss ("1").

7 Legen Sie den Zeitraum fest, in dem die Aktionen auftreten müssen, und klicken Sie dann auf **OK**.



Da es sich um zwei Aktionen handelt, für die Zeitfenster erforderlich sind, müssen Sie den Zehn-Minuten-Zeitraum auf die beiden Aktionen aufteilen. In diesem Beispiel beträgt der Zeitraum für jede Aktion fünf Minuten. Sobald die nicht erfolgreichen Versuche innerhalb von fünf Minuten aufgetreten sind, wird vom System abgehört, ob innerhalb der nächsten fünf Minuten eine erfolgreiche Anmeldung von der gleichen IP-Quelle erfolgt.

8 Klicken Sie im Feld **Gruppieren nach** auf das Symbol, verschieben Sie die Option **Quell-IP** von links nach rechts, was bedeutet, dass alle Aktionen von der gleichen Quell-IP ausgehen müssen. Klicken Sie dann auf **OK**.

9 Definieren Sie die Logik für diese Regel oder Komponente.

Aufgabe	Vorgehensweise
Legen Sie den Typ des Filters fest, durch den die relevanten Ereignisse identifiziert werden (in diesem Fall mehrere fehlgeschlagene Anmeldeversuche bei einem Windows-System).	1 Ziehen Sie das Symbol **Filter** auf das logische Element AND, und legen Sie es dort ab. 2 Klicken Sie auf der Seite **Filterfeldkomponente** auf **Hinzufügen**. 3 Wählen Sie Folgendes aus: **Normalisierungsregel** | **In**aus, und wählen Sie dann Folgendes aus: • **Normalisierung** • **Authentication** • **Anmeldung** • **Host-Anmeldung** • **Mehrere fehlgeschlagene Anmeldeversuche bei einem Windows-Host** 4 Klicken Sie auf **OK**.
Legen Sie fest, wie oft und in welchem Zeitraum die fehlgeschlagene Anmeldung auftreten muss.	1 Ziehen Sie das logische Element **AND** in die Leiste **Filter**, und legen Sie es dort ab. Das Element **AND** wird verwendet, da fünf getrennte Versuche auftreten müssen. Mit dem Element können Sie festlegen, wie oft und in welchem Zeitraum die Versuche auftreten müssen. 2 Klicken Sie auf das Symbol **Menü** für das gerade hinzugefügte Element **AND** und dann auf **Bearbeiten**. 3 Geben Sie in das Feld **Schwellenwert** den Wert **5** ein, und entfernen Sie andere vorhandene Werte. 4 Legen Sie das **Zeitfenster** auf **5** fest. 5 Klicken Sie auf **OK**.
Definieren Sie den zweiten Filtertyp, der auftreten muss (die erfolgreiche Anmeldung).	1 Ziehen Sie das Symbol **Filter** in das untere Ende der eckigen Klammer des ersten logischen Elements **AND**, und legen Sie es dort ab. 2 Klicken Sie auf der Seite **Komponente vergleichen** auf **Hinzufügen**. 3 Wählen Sie in den Feldern die Optionen **Normalisierungsregel** | **In**aus, und wählen Sie dann Folgendes aus: • **Normalisierung** • **Authentication** • **Anmeldung** • **Host-Anmeldung** 4 Klicken Sie auf **OK**, um zur Seite **Komponente vergleichen** zurückzukehren. 5 Definieren Sie "erfolgreich", indem Sie auf **Hinzufügen** klicken und dann **Ereignisuntertyp** | **In**auswählen. Klicken Sie dann auf das Symbol **Variablen**, und klicken Sie auf **Ereignisuntertyp** | **Erfolg** | **Hinzufügen**. 6 Klicken Sie auf **OK**, um zum **Richtlinien-Editor** zurückzukehren.

Die neue Regel wird zur Liste der Korrelationsregeln im **Richtlinien-Editor** hinzugefügt.

Hinzufügen oder Bearbeiten einer Datenzugriffsregel

Mithilfe von DEM-Datenzugriffsrichtlinien können Sie unbekannte Zugriffspfade in die Datenbank verfolgen und Ereignisse in Echtzeit senden.

Wenn Sie die richtigen Datenzugriffsrichtlinien erstellen, können Sie allgemeine Verletzungen in Datenbankumgebungen leicht verfolgen, beispielsweise Anwendungsentwickler, die mit Anmelde-IDs für Anwendungen auf Produktionssysteme zugreifen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** Folgendes aus: **DEM** | **Datenzugriff**.

2 Führen Sie einen der folgenden Schritte aus:

- Zum Hinzufügen einer neuen Regel wählen Sie **Neu** aus, und klicken Sie dann auf **Datenzugriffsregel**
- Zum Bearbeiten einer Regel wählen Sie die Regel im Regelanzeigebereich aus, und klicken Sie dann auf **Bearbeiten** | **Ändern**.

3 Geben Sie die Informationen ein, und klicken Sie dann auf **OK**.

Hinzufügen oder Bearbeiten einer Transaktionsüberwachungsregel

Mit Transaktionsüberwachungsregeln können Sie Datenbanktransaktionen verfolgen und Änderungen automatisch abgleichen sowie Start und Ende einer Handelsausführung oder Begin- und Commit-Anweisungen protokollieren, um Berichte nach Transaktionen anstelle von Abfragen zu erstellen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** Folgendes aus: **DEM** | **Transaktionsüberwachung**.

2 Führen Sie einen der folgenden Schritte aus:

- Zum Hinzufügen einer neuen Regel klicken Sie auf **Neu** und dann auf **Transaktionsüberwachungsregel**.
- Zum Bearbeiten einer Regel wählen Sie die Regel im Regelanzeigebereich aus, und klicken Sie dann auf **Bearbeiten** | **Ändern**.

3 Geben Sie die Informationen ein, und klicken Sie dann auf **OK**.

Verwalten benutzerdefinierter ADM-Regeln, DEM-Regeln oder Korrelationsregeln

Kopieren Sie eine vordefinierte Regel, und verwenden Sie diese als Vorlage für eine benutzerdefinierte Regel. Beim Hinzufügen einer benutzerdefinierten Regel können Sie die Einstellungen bearbeiten, kopieren und einfügen, um die Regel als Vorlage für eine neue benutzerdefinierte Regel zu verwenden, oder die Einstellungen löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** die Option **ADM** oder **DEM** | **Database**, **Datenzugriff** oder **Transaktionsüberwachung** aus.

2 Führen Sie einen oder mehrere der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Anzeigen aller benutzerdefinierten ADM- oder DEM-Regeln	1 Wählen Sie im Bereich **Filter/Kennzeichnung** die Registerkarte **Filter** aus. 2 Klicken Sie unten im Bereich auf die Leiste **Erweitert**. 3 Wählen Sie im Feld **Herkunft** die Option **benutzerdefiniert** aus. 4 Klicken Sie auf **Abfrage ausführen**. Die benutzerdefinierten Regeln des ausgewählten Typs werden im Regelanzeigebereich aufgeführt.
Kopieren und Einfügen einer Regel	1 Wählen Sie eine vordefinierte oder benutzerdefinierte Regel aus. 2 Klicken Sie auf **Bearbeiten** | **Kopieren** 3 Klicken Sie auf **Bearbeiten** | **Einfügen**. Die kopierte Regel wird zur Liste der vorhandenen Regeln unter dem gleichen Namen hinzugefügt. 4 Zum Ändern des Namens klicken Sie auf **Bearbeiten** | **Ändern**.
Ändern einer benutzerdefinierten Regel	1 Wählen Sie die benutzerdefinierte Regel aus. 2 Klicken Sie auf **Bearbeiten** | **Ändern**.
Löschen einer benutzerdefinierten Regel	1 Wählen Sie die benutzerdefinierte Regel aus. 2 Klicken Sie auf **Bearbeiten** | **Löschen**.

Einrichten einer Regel und eines Berichts für Datenbank-Audit-Listen

Im Bericht **Audit-Listen für berechtigte Benutzer** können Sie die Audit-Liste für Änderungen an der Datenbank anzeigen oder den Zugriff auf eine Datenbank oder Tabelle verfolgen, der einem bestimmten Datenbankereignis zugeordnet war.

Wenn Sie die Parameter zum Generieren des Berichts eingerichtet haben, erhalten Sie Benachrichtigungen über Compliance-Berichte, in denen die dem jeweiligen Ereignis zugeordnete Audit-Liste angezeigt wird. Zum Generieren der Audit-Listenereignisse müssen Sie eine Regel für den **Datenzugriff** und den Bericht **Audit-Listen für berechtigte Benutzer** hinzufügen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** Folgendes aus: **DEM** | **Datenzugriff**.

2 Heben Sie im Regelanzeigebereich die Optionen **DEM – Vorlagenregel – Zugriff durch vertrauenswürdige Verwendung aus IP-Bereich** hervor.

3 Klicken Sie auf **Bearbeiten** | **Kopieren**und dann auf **Bearbeiten** | **Einfügen**.

4 Ändern Sie den Namen und die Eigenschaften der neuen Regel.

   a Heben Sie die neue Regel hervor, und wählen Sie dann Folgendes aus: **Bearbeiten** | **Ändern**.

   b Geben Sie einen Namen für die Regel und dann den Benutzernamen ein.

   c Wählen Sie den Aktionstyp **Nicht vertrauenswürdig** aus, und klicken Sie dann auf **OK**.

5 Klicken Sie auf das Symbol **Rollout**  .

6 Richten Sie den Bericht ein:

a Klicken Sie in **Systemeigenschaften** auf **Berichte** | **Hinzufügen**.

b Füllen Sie die Abschnitte 1 – 3 und 6 aus.

c Wählen Sie in Abschnitt 4 die Option **Bericht im PDF-Format** oder **Bericht im HTML-Format** aus.

d Wählen Sie in Abschnitt 5 die Optionen **Compliance** | **SOX** | **Audit-Listen für berechtigte Benutzer (Datenbank) aus.**.

e Klicken Sie auf **Speichern**.

7 Zum Generieren des Berichts klicken Sie auf **Jetzt ausführen**.

ESM-Regeln

ESM-Regeln werden verwendet, um Ereignisse im Zusammenhang mit dem ESM-Gerät zu generieren.

Alle Regeln dieses Typs werden von McAfee definiert. Sie können verwendet werden, um Compliance- oder Audit-Berichte zu generieren, aus denen die auf dem ESM-Gerät aufgetretenen Ereignisse hervorgehen. Sie können diese Regeln nicht hinzufügen, ändern oder löschen. Sie können jedoch die Eigenschaftseinstellungen ändern (siehe *Regeltypen und ihre Eigenschaften*).

Normalisierung

Die Namen und Beschreibungen der Regeln werden von den jeweiligen Anbietern festgelegt. Daher haben Regeln des gleichen Typs oft unterschiedliche Namen. Dies erschwert das Sammeln von Informationen für die auftretenden Ereignistypen.

McAfee hat eine kontinuierlich aktualisierte Liste mit normalisierten IDs zusammengestellt, in der Regeln beschrieben werden, sodass Ereignisse in sinnvollen Kategorien gruppiert werden können. Wenn Sie im **Richtlinien-Editor** im Bereich **Regeltypen** auf **Normalisierung** klicken, werden diese IDs, Namen und Beschreibungen angezeigt.

Bei den folgenden Ereignisfunktionen können Sie Ereignisinformationen mithilfe normalisierter IDs organisieren:

- Felder von Ansichtskomponenten: **Normalisierte Ereigniszusammenfassung** ist eine Option beim Definieren von Feldern für eine Ereignisabfrage in den Komponenten Kreisdiagramm, Balkendiagramm und Liste (siehe *Verwalten von Abfragen*).
- Filter für Ansichtskomponenten: Beim Erstellen einer neuen Ansicht können Sie auswählen, dass Ereignisdaten in einer Komponente anhand der normalisierten IDs gefiltert werden sollen (siehe *Verwalten von Abfragen*).
- Ansichtsfilter: **Normalisierte ID** ist eine Option in der Liste der Ansichtsfilter (siehe *Filtern von Ansichten*).
- Ansichtsliste: Die Ansicht **Normalisierte Ereigniszusammenfassung** ist in der Liste der **Ereignisansichten** verfügbar.

Auf der Registerkarte **Details** in der Ansicht **Ereignisanalyse** werden die Normalisierungs-IDs für die in der Liste angezeigten Ereignisse aufgeführt.

Beim Hinzufügen von Filtern für **Normalisierte ID** zu einer neuen oder vorhandenen Ansicht haben Sie folgende Möglichkeiten:

- Filtern Sie nach allen normalisierten IDs in einem Ordner der ersten Ebene. Am Ende der ID ist eine Maske (/5 für einen Ordner der ersten Ebene) enthalten. Daran erkennen Sie, dass die Ereignisse außerdem nach den untergeordneten IDs des ausgewählten Ordners gefiltert werden.
- Filtern Sie nach den IDs in einem Ordner der zweiten oder dritten Ebene. Am Ende der ID ist eine Maske (/12 für einen Ordner der zweiten Ebene, /18 für einen Ordner der dritten Ebene) enthalten. Daran erkennen Sie, dass die Ereignisse nach den untergeordneten IDs des ausgewählten Unterordners gefiltert werden. Die vierte Ebene hat keine Maske.
- Filtern Sie nach einer einzelnen ID.
- Filtern Sie nach mehreren Ordnern oder IDs gleichzeitig, indem Sie beim Auswählen der Ordner oder IDs die **STRG**-Taste oder die **UMSCHALTTASTE** gedrückt halten.

Aktivieren von Paket kopieren

Wenn **Paket kopieren** für eine Regel aktiviert ist, werden die Paketdaten auf das ESM-Gerätekopiert. Wenn die Option aktiviert ist, sind Paketdaten in den Quellereignisdaten eines Alarms vom Typ **Interne Ereignisübereinstimmung** oder **Feldübereinstimmung** enthalten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ESM-Konsole auf das Symbol **Richtlinien-Editor** .

2 Klicken Sie im Bereich **Regeltypen** auf den Typ der Regel, auf die Sie zugreifen möchten. Suchen Sie dann die Regel im Regelanzeigebereich.

3 Klicken Sie in der Spalte **Paket kopieren** auf die aktuelle Einstellung (standardmäßig **aus**), und klicken Sie dann auf **an**.

Einstellungen für Standardrichtlinien

Sie können die Standardrichtlinie so einrichten, dass sie im reinen Warnungsmodus oder im Überbelegungsmodus verwendet wird. Außerdem können Sie den Status der Regelaktualisierungen anzeigen und eine Aktualisierung initiieren.

Reiner Warnungsmodus

Richtlinien können auf Nitro IPS und auf virtuelle Geräte angewendet werden, für die **Reiner Warnungsmodus** aktiviert ist.

Wenn **Reiner Warnungsmodus** aktiviert ist, werden alle aktivierten Regeln an die Geräte mit Warnungen gesendet. Dies gilt auch, wenn die Regel auf eine Blockierungsaktion wie **Verwerfen** festgelegt ist. Beim Anzeigen der generierten Ereignisse wird in der Spalte **Ereignisuntertyp** die Aktion **Warnung** aufgeführt, gefolgt von der ausgeführten Aktion, wenn **Reiner Warnungsmodus** nicht aktiv war, beispielsweise **Warnung und verwerfen**. Dies ist hilfreich für Systemadministratoren, die noch dabei sind, sich mit den Verkehrsmustern im Netzwerk vertraut zu machen. Sie können generierte Ereignisse analysieren, ohne aktiv Ereignisse zu blockieren, und sehen dennoch die Aktion, die ausgeführt wird, wenn **Reiner Warnungsmodus** aktiviert ist.

Durch Aktivieren von **Reiner Warnungsmodus** werden keine einzelnen Verwendungseinstellungen für einzelne Regeln im **Richtlinien-Editor** geändert. Beispiel: Wenn der Modus aktiviert ist, kann eine Regel mit Warnungen an das Nitro IPS-Gerät oder das virtuelle Gerät gesendet werden, obwohl die Verwendung im **Richtlinien-Editor** auf **Verwerfen** festgelegt ist. (Ausnahme: Eine auf **Zulassen** festgelegte Regel bleibt in diesem Modus.) Auf diese Weise können Sie problemlos **Reiner Warnungsmodus** aktivieren und

deaktivieren, ohne dass sich dies anderweitig auf die Richtlinieneinstellungen auswirkt. **Reiner Warnungsmodus** hat keine Auswirkungen auf deaktivierte Regeln. Wenn **Deaktivieren** festgelegt ist, werden Regeln nie an ein Gerät gesendet.

Aktivieren von Reiner Warnungsmodus

Wenn Sie möchten, dass alle aktivierten Regeln mit Warnungen an die Geräte gesendet werden, müssen Sie die Funktion **Reiner Warnungsmodus** aktivieren. Da für diese Einstellung die Vererbung gilt, wird mit der Einstellung dieser Richtlinie der Wert überschrieben, den sie anderenfalls erben würde.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** auf das Symbol **Einstellungen**  .
2. Wählen Sie im Feld **Reiner Warnungsmodus** die Option **An** aus.

Einrichten des Überbelegungsmodus

Mit dem **Überbelegungsmodus** definieren Sie, wie Pakete bei Überschreitung der Gerätekapazität behandelt werden. Das Paket wird jeweils als Ereignis aufgezeichnet.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** auf das Symbol **Einstellungen**  .
2. Klicken Sie im Feld **Überbelegungsmodus** auf **Aktualisieren**.
3. Geben Sie in das Feld **Wert** die Funktionalität ein.
   a. Mit Zulassen (pass oder 1) lassen Sie zu, dass Pakete, die sonst verworfen würden, ohne Scannen weitergeleitet werden.
   b. Mit Verwerfen (drop oder 0) werden Pakete, durch die die Gerätekapazität überschritten wird, verworfen.
   c. Um ein Paket ohne Generieren eines Ereignisses zuzulassen oder zu verwerfen, geben Sie `spass` oder `sdrop` ein.
4. Klicken Sie auf **OK**.



Ab Version 8.1.0 wirken sich Änderungen am **Überbelegungsmodus** auf das Gerät und seine untergeordneten Geräte (virtuelle Geräte) aus. Damit die Änderung wirksam wird, müssen Sie den Modus auf dem übergeordneten Gerät ändern.

Anzeigen des Richtlinienaktualisierungsstatus für Geräte

Zeigen Sie eine Zusammenfassung des Status von Richtlinienaktualisierungen für alle Geräte in ESM an.

So können Sie ermitteln, wann Sie einen Rollout für Aktualisierungen auf dem System ausführen müssen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im **Richtlinien-Editor** auf das Symbol **Einstellungen**  .

2 Im Feld **Status** wird die Anzahl der Geräte angezeigt, die aktuell oder veraltet sind und für die ein automatischer Rollout geplant ist.

3 Klicken Sie auf **Schließen**.

Regelvorgänge

Sie können verschiedene Vorgänge für die Regeln ausführen, um sie zu verwalten und die benötigten Informationen zu generieren.

Verwalten von Regeln

Sie können Regeln für **ADM**, **DEM**, **Deep Packet Inspection**, den **Erweiterten Syslog-Parser** und die **Korrelation** anzeigen, kopieren und einfügen. Benutzerdefinierte Regeln dieser Typen können geändert oder gelöscht werden. Standardregeln können geändert werden, müssen aber als neue benutzerdefinierte Regel gespeichert werden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** den Typ der Regel aus, mit der Sie arbeiten möchten.

2 Führen Sie einen oder mehrere der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Anzeigen benutzerdefinierter Regeln	1 Wählen Sie im Bereich **Filter/Kennzeichnung** die Registerkarte **Filter** aus. 2 Klicken Sie unten im Bereich auf die Leiste **Erweitert**. 3 Wählen Sie im Feld **Herkunft** die Option **benutzerdefiniert** aus, und klicken Sie dann auf **Abfrage ausführen**  .
Kopieren und Einfügen einer Regel	1 Wählen Sie eine vordefinierte oder benutzerdefinierte Regel aus. 2 Wählen Sie Folgendes aus: **Bearbeiten** | **Kopieren**aus, und wählen Sie dann Folgendes aus: **Bearbeiten** | **Einfügen**. Die kopierte Regel wird zur Liste der vorhandenen Regeln unter dem gleichen Namen hinzugefügt. 3 Zum Ändern des Namens wählen Sie Folgendes aus: **Bearbeiten** | **Ändern**.

Aufgabe	Vorgehensweise
Ändern einer Regel	1 Heben Sie die Regel hervor, die Sie anzeigen möchten, und wählen Sie dann Folgendes aus: **Bearbeiten** | **Ändern**. 2 Ändern Sie die Einstellungen, und klicken Sie dann auf **OK**. Wenn es sich um eine benutzerdefinierte Regel handelt, wird diese mit den Änderungen gespeichert. Bei einer Standardregel werden Sie aufgefordert, die Änderungen als neue benutzerdefinierte Regel zu speichern. Klicken Sie auf **Ja**. Wenn Sie den Namen der Regel nicht geändert haben, wird sie unter dem gleichen Namen und mit einer anderen Signatur-ID gespeichert. Sie können den Namen ändern, indem Sie die Regel auswählen und dann Folgendes auswählen: **Bearbeiten** | **Ändern**.
Löschen einer benutzerdefinierten Regel	• Wählen Sie die benutzerdefinierte Regel aus. • Wählen Sie Folgendes aus: **Bearbeiten** | **Löschen**.

Importieren von Regeln

Sie können einen von einem anderen ESM-Gerät exportierten Regelsatz importieren und auf Ihrem ESM-Gerät speichern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im **Richtlinien-Editor** im Bereich **Regeltypen** auf den Typ der zu importierenden Richtlinien oder Regeln.

2 Klicken Sie auf **Datei** | **Importieren**, und wählen Sie dann die Option **Regeln** aus.

Diese Änderungen werden nicht verfolgt und können daher nicht rückgängig gemacht werden.

3 Klicken Sie auf **Regeln importieren**, navigieren Sie dann zu der zu importierenden Datei, und wählen Sie die Option **Hochladen** aus.

Die Datei wird in das ESM-Gerät hochgeladen.

4 Wählen Sie auf der Seite **Regeln importieren** die Aktion aus, die ausgeführt werden soll, wenn importierte Regeln die gleiche ID haben wie vorhandene Regeln.

5 Klicken Sie auf **OK**, um die Regeln zu importieren, und beheben Sie die Konflikte gemäß den Hinweisen.

Der Inhalt der Datei wird überprüft, und abhängig vom Inhalt der ausgewählten Datei werden die entsprechenden Optionen aktiviert bzw. deaktiviert.

Konflikte beim Importieren von Korrelationsregeln

Beim Exportieren von Korrelationsregeln wird eine Datei erstellt, die die Regeldaten enthält. Die Datei enthält jedoch keine referenzierten Elemente wie beispielsweise Variablen, Zonen,

Überwachungslisten, benutzerdefinierte Typen und Ressourcen, die möglicherweise von dieser Regel verwendet werden.

Wenn Sie die Exportdatei auf einem anderen ESM-Gerät importieren, führen alle in der Regel enthaltenen referenzierten Elemente, die auf dem importierenden System nicht vorhanden sind, zu einem Regelkonflikt. Wenn beispielsweise Regel 1 auf die Variable $abc verweist und auf dem importierenden System keine Variable mit dem Namen $abc definiert ist, stellt dies einen Konflikt dar. Konflikte werden protokolliert, und die Regel wird als in Konflikt stehend gekennzeichnet.

Konflikte können Sie beheben, indem Sie die benötigten referenzierten Elemente (manuell oder gegebenenfalls durch Importieren) erstellen oder die Korrelationsregel bearbeiten und die Verweise innerhalb der Regel ändern.

Wenn Regeln mit Konflikten vorhanden sind, wird unmittelbar nach dem Importvorgang eine Seite angezeigt, aus der hervorgeht, welche Regeln in Konflikt stehen oder fehlgeschlagen sind. Sie können auf dieser Seite Regeln bearbeiten, um Konflikte zu beheben, oder die Seite schließen. Regeln mit Konflikten sind mit einem Ausrufezeichensymbol gekennzeichnet, das ihren Status angibt. Beim Bearbeiten einer in Konflikt stehenden Regel im Regel-Editor wird eine Schaltfläche für Konflikte angezeigt. Wenn Sie auf diese Schaltfläche klicken, werden die Konfliktdetails für die jeweilige Regel angezeigt.

Importieren von Variablen

Sie können eine Datei mit Variablen importieren und deren Typ ändern. Bei Konflikten wird die neue Variable automatisch umbenannt.

Bevor Sie beginnen

Richten Sie die zu importierende Datei ein.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** im Bereich **Regeltypen** auf **Variable**.
2. Klicken Sie auf **Datei** | **Importieren** | **Variablen**, navigieren Sie dann zu der Datei mit den Variablen, und klicken Sie auf **Hochladen**.

   Bei Konflikten oder Fehlern in der Datei wird die Seite **Import: Fehlerprotokoll** geöffnet, auf der Sie über die einzelnen Probleme informiert werden.
3. Klicken Sie auf der Seite **Variablen importieren** auf **Bearbeiten**, um den **Typ** für die ausgewählten Variablen zu ändern.
4. Klicken Sie auf **OK**.

Exportieren von Regeln

Exportieren Sie benutzerdefinierte Regeln oder alle Regeln in einer Richtlinie, und importieren Sie sie dann auf einem anderen ESM-Gerät.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** im Bereich **Regeltypen** auf den Typ der zu exportierenden Regeln.
2. Greifen Sie auf eine Liste der benutzerdefinierten Regeln des ausgewählten Typs zu:
   a. Stellen Sie im Bereich **Filter/Kennzeichnung** sicher, dass die Registerkarte **Filter** ausgewählt ist.
   b. Klicken Sie unten im Bereich auf die Leiste **Erweitert**.
   c. Wählen Sie in der Dropdown-Liste **Herkunft** die Option **benutzerdefiniert** aus.
   d. Klicken Sie auf das Symbol **Abfrage ausführen**  .
3. Wählen Sie die zu exportierenden Regeln aus, und klicken Sie dann auf **Datei** | **Exportieren** | **Regeln**.
4. Wählen Sie auf der Seite **Regeln exportieren** das Format aus, das beim Exportieren der Regel verwendet werden soll.
5. Klicken Sie auf der Seite **Herunterladen** auf **Ja**, wählen Sie den Speicherort aus, und klicken Sie dann auf **Speichern**.



Wenn Sie die CSV-Datei in Microsoft Excel öffnen, sind möglicherweise einige der UTF-8-Zeichen beschädigt. Beheben Sie das Problem, indem Sie in Excel den **Textkonvertierungs-Assistenten** öffnen und die Optionen **Getrennt** und **Komma** auswählen.

Festlegen der automatischen Aufnahme in die Blacklist durch Regeln

Sie können Regeln für die automatische Aufnahme in die Blacklist markieren. Die IP-Adresse bzw. die IP-Adresse und der Port des Angreifers werden zur Blacklist hinzugefügt, wenn die definierten Bedingungen erfüllt sind.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Erweitern Sie im **Richtlinien-Editor** im Bereich **Regeltypen** die Option **IPS**, und wählen Sie dann den Typ der Regel aus. Wenn Sie beispielsweise die automatische Aufnahme in die Blacklist für Virenregeln festlegen möchten, wählen Sie **Deep Packet Inspection** aus.
2. Wählen Sie im Bereich **Filter/Kennzeichnung** auf der Registerkarte **Filter** den Filter aus. Im oben genannten Beispiel würden Sie die Option **Virus** auswählen.
3. Klicken Sie auf das Symbol **Aktualisieren**.

   Die gefilterten Regeln werden im Regelanzeigebereich aufgeführt.
4. Klicken Sie auf die Kopfzeile der Spalte **Blacklist**, oder wählen Sie Regeln in der Liste aus. Klicken Sie dann auf **IP** oder **IP und Port**.
5. Führen Sie einen Rollout für die Änderungen aus, indem Sie in der rechten oberen Ecke auf das Symbol **Rollout**  klicken. Schließen Sie dann den **Richtlinien-Editor**.
6. Wählen Sie in der Systemnavigationsstruktur ein Nitro IPS-Gerät oder ein virtuelles Gerät aus, und klicken Sie dann auf das Symbol **Eigenschaften**  .

7 Klicken Sie auf **Blacklist** und dann auf **Einstellungen**.

8 Definieren Sie auf der Seite **Einstellungen für die automatische Aufnahme in die Blacklist** die Einstellungen, und klicken Sie dann auf **OK**.

Filtern vorhandener Regeln

Wenn Sie im **Richtlinien-Editor** einen Regeltyp auswählen, werden alle Regeln des ausgewählten Typs standardmäßig in alphabetischer Reihenfolge aufgeführt. Sie können die Regeln nach der Uhrzeit anzeigen oder sie mithilfe von Tags filtern, um nur die Ihren Kriterien entsprechenden anzuzeigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** den zu filternden Regeltyp aus.

2 Stellen Sie sicher, dass im Bereich **Filter/Kennzeichnung** die Registerkarte **Filter** ausgewählt ist.

3 Führen Sie einen oder mehrere der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Filtern mit mehreren Tags	• Wählen Sie Kategorien oder Tags aus, und klicken Sie dann auf das Symbol **Abfrage ausführen**  . Daraufhin werden nur Regeln angezeigt, die allen Filtern entsprechen.
Anzeigen von Regeln, die einem der ausgewählten Filter entsprechen	1 Wählen Sie mehrere Kategorien oder Tags aus. 2 Klicken Sie auf das Symbol **oder** und dann auf das Symbol **Abfrage ausführen**.  Von Vererbung betroffene Felder (**Aktion**, **Schweregrad**, **Blacklist**, **Aggregation** und **Paket kopieren**) können nicht über das Symbol **oder** gefiltert werden.
Suchen nach einem bestimmten Tag	1 Geben Sie den Namen des Tags in das Feld **Geben Sie hier Text ein, um nach einem Tag zu suchen** ein. 2 Wählen Sie in der Liste der Optionen die gewünschte Option aus.
Aufführen der Regeln nach dem Zeitpunkt der Erstellung	• Klicken Sie auf der Symbolleiste auf das Symbol **Nach Uhrzeit sortieren**  und dann auf das Symbol **Abfrage ausführen**.
Aufführen der Regeln in alphabetischer Reihenfolge	• Klicken Sie auf der Symbolleiste auf das Symbol **Nach Namen sortieren**  und dann auf das Symbol **Abfrage ausführen**.
Löschen der Filterung	• Klicken Sie auf das orangefarbige Filtersymbol auf der Titelleiste des Regelanzeigebereichs  . Die Filter werden gelöscht, und alle Regeln werden wieder im Regelanzeigebereich angezeigt.
Löschen der Filter-Tags	• Klicken Sie auf der Symbolleiste auf das Symbol **Alle löschen**  . Tags werden gelöscht, die Liste der Regel bleibt jedoch gefiltert.

Aufgabe	Vorgehensweise
Filtern nach Signatur-ID	1 Klicken Sie unten im Bereich **Filter** auf die Leiste **Erweitert**. 2 Geben Sie die Signatur-ID ein, und klicken Sie dann auf das Symbol **Abfrage ausführen**.
Filtern nach Name oder Beschreibung	1 Geben Sie im Bereich **Erweitert** den Namen oder die Beschreibung ein. 2 Wenn die Ergebnisse ungeachtet der Groß-/Kleinschreibung angezeigt werden sollen, klicken Sie auf das Symbol Groß-/Kleinschreibung ignorieren Aa.
Filtern nach Gerätetyp, normalisierter ID oder Aktion	1 Klicken Sie im Bereich **Erweitert** auf das Symbol **Filter** . 2 Wählen Sie auf der Seite **Filtervariablen** die Variable aus.
Vergleichen Sie die Unterschiede in den richtlinienbasierten Einstellungen für einen Regeltyp und dessen unmittelbar übergeordneten Regeltyp.	• Wählen Sie im Bereich **Erweitert** die Option **Ausnahmen anzeigen** aus, und klicken Sie dann auf das Symbol **Abfrage ausführen**.
Filtern nach Schweregrad, Blacklist, Aggregation, Paket kopieren, Herkunft und Regelstatus	• Wählen Sie den Filter in der Dropdown-Liste in jedem dieser Felder aus.
Anzeigen nur benutzerdefinierter Regeln	• Wählen Sie im Bereich **Erweitert** im Feld **Herkunft** die Option **benutzerdefiniert** aus, und klicken Sie dann auf das Symbol **Abfrage ausführen**.
Anzeigen von Regeln, die in einem bestimmten Zeitraum erstellt wurden	1 Klicken Sie im Bereich **Erweitert** auf das Kalendersymbol neben dem Feld **Uhrzeit**. 2 Wählen Sie auf der Seite **Benutzerdefinierter Zeitpunkt** die Start- und Endzeit aus, klicken Sie auf **OK** und dann auf das Symbol **Abfrage ausführen**.

Anzeigen der Signatur einer Regel

Wenn Sie auf die online verfügbare McAfee-Signaturdatenbank zugreifen, können Sie Informationen zur Signatur einer Regel anzeigen. Diese Option ist für Firewall-Regeln, Deep Packet Inspection-Regeln und Datenquellenregeln verfügbar.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** den Regeltyp aus, den Sie anzeigen möchten.

2 Wählen Sie im Regelanzeigebereich eine Regel aus.

3 Klicken Sie auf **Vorgänge**, und wählen Sie dann **Referenz durchsuchen** aus.

Im Browser wird der Bildschirm **NTAC: Zusammenfassung für Schwachstellen** geöffnet.

4 Zum Anzeigen der Zusammenfassung einer Signatur klicken Sie auf die Links im Bildschirmabschnitt **Signaturen**.

Abrufen von Regelaktualisierungen

Die von einem Nitro IPS-Gerät oder einem virtuellen Gerät für die Untersuchung des Netzwerkverkehrs verwendeten Regelsignaturen werden vom für Signaturen zuständigen McAfee-Team ständig aktualisiert und stehen auf dem zentralen Server als Download zur Verfügung. Die Regelaktualisierungen können automatisch oder manuell abgerufen werden.

Vorgehensweise

Informationen zum Einrichten von Überschreibungen für die Aktionen, die beim Abruf der Regeln vom Server ausgeführt werden, finden Sie unter *Überschreibungsaktion für heruntergeladene Regeln*.

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** auf das Symbol **Einstellungen** .
2. Klicken Sie in der Zeile **Regelaktualisierung** auf **Aktualisieren**.
3. Legen Sie fest, dass die Aktualisierungen automatisch vom ESM-Gerät abgerufen werden, oder führen Sie die Überprüfung auf Aktualisierungen sofort aus.
4. Wenn Aktualisierungen manuell heruntergeladen wurden, klicken Sie auf das Symbol **Rollout** , um sie anzuwenden.
5. Zum Anzeigen der manuellen Aktualisierungen führen Sie die folgenden Schritte aus:
   a. Klicken Sie im Bereich **Filter/Kennzeichnung** auf die Leiste **Erweitert**.
   b. Wählen Sie im Feld **Regelstatus** die Option **aktualisiert**, **neu** oder **aktualisiert/neu** aus, um den Typ der anzuzeigenden Regeln anzugeben.
   c. Klicken Sie auf das Symbol **Abfrage ausführen** .

Die aktualisierten Regeln werden mit einem Sternenregensymbol aufgeführt, wenn sie hinzugefügt wurden, bzw. mit einem Ausrufezeichen , wenn sie geändert wurden.

Löschen des aktualisierten Regelstatus

Wenn Regeln geändert oder zum System hinzugefügt werden, und Sie Gelegenheit hatten, die Aktualisierungen zu überprüfen, können Sie diese Markierungen löschen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** den Typ der zu löschenden Regel aus.
2. Führen Sie einen der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Löschen aller Markierungen für den Regelstatus	1 Klicken Sie auf **Vorgänge**, und wählen Sie dann **Aktualisierten Regelstatus löschen** aus. 2 Klicken Sie auf **Alle**.
Löschen ausgewählter Regeln	1 Klicken Sie im Bereich **Filter/Kennzeichnung** auf die Leiste **Erweitert**. 2 Wählen Sie im Feld **Regelstatus** die Option **aktualisiert**, **neu** oder **aktualisiert/neu** aus, um den Typ der zu löschenden Markierung anzugeben. 3 Klicken Sie auf das Symbol **Abfrage ausführen**. Die Regeln mit den ausgewählten Markierungen werden im Regelanzeigebereich aufgeführt. 4 Wählen Sie die zu löschenden Regeln aus. 5 Klicken Sie auf **Vorgang** | **Aktualisierten Regelstatus löschen** | **Ausgewählt**.

Vergleichen von Regeldateien

Sie können den Richtlinienstatus (angewendet, aktuell, Rollback oder bereitgestellt) von Regeldateien für Nitro IPS, Empfänger, ADM und DEM vergleichen.
Dies ist hilfreich, wenn Sie sehen möchten, was sich durch die Anwendung der aktuellen Richtlinie auf ein Gerät ändern würde. In diesen Fall würden Sie die aktuellen Regeln und die angewendeten Regeln vergleichen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der Systemnavigationsstruktur auf ein Nitro IPS-Gerät, Empfängergerät, ADM- oder DEM-Gerät.

2 Klicken Sie auf der Aktionssymbolleiste auf das Symbol **Richtlinien-Editor** und dann auf **Extras** \| **Regeldateien vergleichen**.

3 Wählen Sie die entsprechenden Optionen aus, zeigen Sie die Ergebnisse an, und klicken Sie dann auf **Schließen**.

Anzeigen des Verlaufs der Regeländerungen

Sie können die geänderten, aktualisierten oder zum System hinzugefügten Regeln sowie die neueste Version der jeweiligen Regel anzeigen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im **Richtlinien-Editor** auf **Extras** \| **Verlauf der Regeländerungen**.

2 Zeigen Sie auf der Seite **Regelverlauf** die an Regeln vorgenommenen Änderungen an, oder klicken Sie auf die Registerkarte **Regelversion**, um die neueste Version der jeweiligen Regel anzuzeigen.

3 Klicken Sie auf **Schließen**.

Erstellen einer neuen Überwachungsliste mit Regeln

Eine Überwachungsliste ist eine Gruppierung bestimmter Informationstypen, die Sie als Filter oder Alarmbedingung verwenden können, damit Sie benachrichtigt werden, wenn diese in einem Ereignis

auftreten. Die Überwachungslisten können global oder spezifisch für einzelne ESM-Benutzer oder -Gruppen gelten.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** den Typ der Regel aus. Wählen Sie dann die Regeln aus, die in der Überwachungsliste enthalten sein sollen.

2 Klicken Sie auf **Vorgänge**, und wählen Sie dann die Option **Neue Überwachungsliste erstellen** aus.

Die ausgewählten Regeln werden auf der Seite **Überwachungsliste hinzufügen** aufgeführt.

3 Geben Sie einen Namen ein, und stellen Sie dann sicher, dass die Optionsschaltfläche **Statisch** ausgewählt ist.

Informationen zum Hinzufügen einer dynamischen Überwachungsliste finden Sie unter *Hinzufügen einer neuen Überwachungsliste*.

4 Wählen Sie den Typ der Daten aus, die mit der Überwachungsliste überwacht werden sollen, und wählen Sie dann den Beauftragten aus.

Ein Benutzer mit Administratorberechtigungen kann eine Überwachungsliste einem belieben Benutzer oder einer beliebigen Gruppe im System zuweisen. Wenn Sie nicht über Administratorberechtigungen verfügen, können Sie Überwachungslisten nur sich selbst oder Gruppen, in denen Sie Mitglied sind, zuweisen.

5 Wenn Sie weitere Werte zur Watchlist hinzufügen möchten, haben Sie folgende Möglichkeiten:

- Zum Importieren einer Datei mit Werten im durch neue Zeilen getrennten Format klicken Sie auf **Importieren**, und wählen Sie dann die Datei aus.
- Zum Hinzufügen einzelner Werte geben Sie im Feld **Werte** einen Wert pro Zeile ein.

Es sind maximal 1.000 Werte möglich.

6 Um einen Alarm zu erhalten, sobald ein Ereignis generiert wird, das einen der Werte aus der Watchlist enthält, klicken Sie auf **Alarm erstellen**.

7 Klicken Sie auf **OK**.

Hinzufügen von Regeln zu einer Überwachungsliste

Wenn Sie eine Überwachungsliste erstellt haben, müssen Sie möglicherweise Regelwerte hinzufügen. Dazu können Sie die Option **An Überwachungsliste anfügen** verwenden.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** den Typ der Regel aus.

2 Wählen Sie im Regelanzeigebereich die Regeln aus, die Sie an die Überwachungsliste anfügen möchten.

3 Klicken Sie auf das Menü **Vorgänge**, und wählen Sie dann **An Überwachungsliste anfügen** aus.

4 Wählen Sie die Überwachungsliste aus, an die Sie die Regeln einfügen möchten, und klicken Sie auf **OK**.

Zuweisen von Tags zu Regeln oder Ressourcen

Sie können Regeln Tags zuweisen, aus denen ihre Attribute hervorgehen, und dann die Regeln nach den Tags filtern. Auf dem ESM-Gerät befindet sich ein Satz vordefinierter Tags. Sie können jedoch auch neue Tags und Tag-Kategorien hinzufügen.

Die Registerkarte **Tags** ist für die Regeltypen Variable, Präprozessor oder Normalisierung nicht verfügbar.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** den Regeltyp aus, den Sie kennzeichnen möchten.

2 Klicken Sie im Bereich **Filter/Kennzeichnung** auf die Registerkarte **Tags**.

3 Führen Sie einen oder mehrere der folgenden Schritte aus:

Aufgabe	Vorgehensweise
Hinzufügen einer neuen Tag-Kategorie	1 Klicken Sie auf das Symbol **Neues Kategorie-Tag**  . 2 Geben Sie den Namen für die Kategorie ein. 3 Wenn das Tag für Berechnung des Ereignisschweregrads verwendet werden soll, wählen Sie **Tag für Berechnung des Ereignisschweregrads verwenden** aus, und klicken Sie dann auf **OK**. Die Kategorie wird mit einem Basis-Tag hinzugefügt. Sie können unter dieser Kategorie neue Tags hinzufügen.
Hinzufügen eines neuen Tags	1 Klicken Sie auf die Kategorie, zu der Sie das Tag hinzufügen möchten, und dann auf das Symbol **Neues Tag**  . 2 Geben Sie den Namen für das Tag ein. 3 Wenn das Tag für Berechnung des Ereignisschweregrads verwendet werden soll, wählen Sie **Tag für Berechnung des Ereignisschweregrads verwenden** aus, und klicken Sie dann auf **OK**.
Bearbeiten einer vorhandenen Kategorie oder eines vorhandenen Tags	1 Klicken Sie auf die zu bearbeitende Kategorie oder das zu bearbeitende Tag und dann auf das Symbol **Tag bearbeiten**  . 2 Ändern Sie den Namen oder die Einstellung, und klicken Sie dann auf **OK**.
Löschen eines benutzerdefinierten Tags	1 Heben Sie das zu löschende Tag hervor, und klicken Sie dann auf das Symbol **Tag entfernen**  . 2 Klicken Sie zur Bestätigung auf **Ja**.

Aggregationseinstellungen ändern

Aggregierte Ereignisse sind Ereignisse mit übereinstimmenden Feldern.

Die Aggregation ist standardmäßig ausgewählt. Sie können auf der Seite **Ereignisaggregation** für jedes Gerät den Aggregationstyp auswählen, der für alle in einem Gerät generierten Ereignisse verwendet werden soll. Sie können die Aggregationseinstellungen für einzelne Regeln ändern.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Wählen Sie im **Richtlinien-Editor** im Bereich **Regeltypen** den Typ der Regel aus.
2. Wählen Sie die Regel aus, deren Aggregationseinstellungen Sie ändern möchten.
3. Klicken Sie auf der Symbolleiste auf **Vorgänge**, und wählen Sie **Aggregationseinstellungen ändern** aus.
4. Wählen Sie in den Dropdown-Listen **Feld 2** und **Feld 3** die zu aggregierenden Feldtypen aus.

   Die Felder müssen unterschiedliche Typen haben, da ansonsten ein Fehler auftritt.

5. Klicken Sie auf **OK**, um die Einstellungen zu speichern.
6. Wenn Sie Änderungen vorgenommen haben, die sich auf die Aggregation durch die Geräte auswirken, werden Sie gefragt, ob Sie den Rollout für die Änderungen ausführen möchten. Führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf **Ja**.

      Auf der Seite **Rollout der Aggregationsausnahmen** wird der Status der von der Änderung betroffenen Geräte angezeigt. Alle veralteten Geräte sind aktiviert.

   b. Deaktivieren Sie gegebenenfalls die Kontrollkästchen der Geräte, auf die Sie die Änderungen nicht anwenden möchten.

   c. Klicken Sie auf **OK**, um den Rollout für die Änderungen auszuführen.

   In der Spalte **Status** wird der Status der Aktualisierung beim Rollout der Änderungen angezeigt.

Überschreibungsaktion für heruntergeladene Regeln

Wenn Regeln vom zentralen Server bei McAfee heruntergeladen werden, ist den Regeln eine Standardaktion zugewiesen.

Sie können eine Überschreibungsaktion für Regeln des Typs definieren, den Sie beim Herunterladen auswählen. Wenn keine Überschreibungsaktion definiert ist, wird die Standardaktion der Regeln ausgeführt.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** auf **Extras**, und wählen Sie dann **Neue Regelkonfiguration** aus.

   Auf der Seite **Neue Regelkonfiguration** werden die für die **Standardrichtlinie** vorhandenen Überschreibungen aufgeführt.

2. Legen Sie die Einstellungen für die Überschreibungsaktion fest, und klicken Sie dann auf **Schließen**.

Gewichtungen der Schweregrade

Der Ereignisschweregrad wird basierend auf der Gewichtung des Schweregrads von Ressourcen, Tags, Regeln und Schwachstellen berechnet.

Jeder der vier Schweregrade wird bei der endgültigen Berechnung gewichtet. Bei dieser endgültigen Berechnung wird die Summe der einzelnen vier Schweregrade mit ihren jeweiligen Gewichtungen multipliziert. Auf der Seite **Gewichtungen der Schweregrade** werden die Gewichtungen angezeigt, die den Gruppen aus Ressourcen, Tags, Regeln und Schwachstellen zugeordnet sind. Die Summe der Einstellungen muss 100 entsprechen. Wenn Sie eine Einstellung ändern, wirkt sich dies auf einige oder auf alle Einstellungen aus. Nachfolgend werden die einzelnen Schweregradtypen beschrieben:

Schweregradtyp	Beschreibungen
Asset	Eine Ressource ist eine IP-Adresse, die sich optional in einer Zone befindet. Der Ressourcenschweregrad eines Ereignisses wird wie folgt ermittelt: 1 Die Ziel-IP-Adresse und die Zielzone des Ereignisses werden mit allen Ressourcen verglichen. Wenn eine Übereinstimmung vorliegt, wird der Schweregrad dieser Ressource als Ressourcenschweregrad für das Ereignis verwendet. 2 Wenn keine Übereinstimmung mit Ziel-IP-Adresse und Zielzone gefunden wird, werden Quell-IP-Adresse und Quellzone des Ereignisses mit allen Ressourcen verglichen. Wenn eine Übereinstimmung mit Quell-IP-Adresse und Quellzone vorliegt, wird der Schweregrad der Ressource als Ressourcenschweregrad für das Ereignis verwendet. 3 Wenn keine Übereinstimmung gefunden wird, entspricht der Ressourcenschweregrad null.
Tag	Der Tag-Schweregrad wird mithilfe von McAfee-Tags und benutzerdefinierten Tags berechnet. Damit ein Tag in der Berechnung des Schweregrad verwendet wird, muss es sowohl für die Regel als auch für die Ressource des Ereignisses festgelegt sein. Wenn für die Regel oder Ressourcen keine Tags definiert sind oder keine Übereinstimmung mit einer Ressource gefunden wird, entspricht der Tag-Schweregrad null. Für die Berechnung des Tag-Schweregrads wird die Anzahl der übereinstimmenden Regel- und Ressourcen-Tags mit 10 multipliziert. Der Tag-Schweregrad ist auf 100 begrenzt.
Regel	Der Regelschweregrad entspricht dem Schweregrad, der bei der Erstellung des Ereignisses festgelegt wurde. Basiert auf dem im **Richtlinien-Editor** festgelegten Regelschweregrad des Ereignisses sowie auf allen für die Erfassung des Ereignisses konfigurierten Datenanreicherungen.
Schwachstelle	Wenn VA SVE-Informationen für die Ressource und die Regel eines Ereignisses verfügbar sind, wird als Schweregrad der Schwachstelle der höchste Schweregrad aller übereinstimmenden VA SVEs für Ressourcen und Regeln verwendet. Anderenfalls wird null verwendet.

Festlegen der Gewichtungen der Schweregrade

Die Schweregrade von Ressourcen, Tags, Regeln und Schwachstellen werden bei der Berechnung des Ereignisschweregrads gewichtet. Sie müssen diese Schweregrade definieren.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie im **Richtlinien-Editor** auf das Symbol **Gewichtungen der Schweregrade**  .

2 Definieren Sie die Einstellungen, und klicken Sie dann auf **OK**.

Anzeigen des Verlaufs der Richtlinienänderungen

Sie können ein Protokoll der an der Richtlinie vorgenommenen Änderungen anzeigen oder exportieren. Dieses Protokoll kann maximal 1 GB an Daten enthalten. Wenn das Limit erreicht ist, werden die ältesten Dateien nach Bedarf gelöscht.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** auf das Symbol **Verlauf der Richtlinienänderungen anzeigen**  .
2. Zeigen Sie ein Protokoll an, oder exportieren Sie ein Protokoll, und klicken Sie dann auf **Schließen**.

Anwenden von Richtlinienänderungen

Wenn Sie Änderungen an Richtlinien vornehmen, müssen Sie einen Rollout für die Änderungen ausführen, um sie anzuwenden. Änderungen auf der Standardrichtlinienebene werden auf alle Richtlinien angewendet, wenn Sie einen Rollout auf allen Geräten ausführen.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** auf das Symbol **Rollout**  .
2. Wählen Sie aus, wie der Rollout ausgeführt werden soll.
3. Klicken Sie auf **OK**.

Nach Abschluss des Rollouts auf den einzelnen Geräten weist der Status der Richtlinie auf einen erfolgreichen Rollout hin. Wenn der Rollout-Befehl nicht erfolgreich ausgeführt wurde, wird eine Seite mit einer Zusammenfassung der fehlgeschlagenen Befehle angezeigt.

Verwalten von Datenverkehr mit Priorität

Sie können Datenverkehr so einrichten, dass er das Nitro IPS-Gerät passiert, ohne anhand von Regeln getestet zu werden.

Möglicherweise müssen Sie beispielsweise VoIP-Verkehr (Voice over Internet Protocol) so einrichten, dass dieser das Nitro IPS-Gerät ohne Verzögerung durch Überprüfungen passiert.

Vorgehensweise

Beschreibungen der Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie im **Richtlinien-Editor** auf den Regeltyp **Variable**.
2. Erweitern Sie die Kategorie **priority_traffic**, und klicken Sie dann auf **PRIORITY_TRAFFIC_LIST**.
3. Klicken Sie auf **Bearbeiten**, und wählen Sie dann **Ändern** aus.
4. Verwalten Sie die Einstellungen, und klicken Sie dann auf **OK**.

Index

A

Abfragen
- Löschen, ausgeführt 215, 216
- Verwalten 215, 216

Abfragen-Assistent 290
Abrufen von Regelaktualisierungen 369
ACE
- Auswählen des Datentyps zum Senden von ESM 137
- Hinzufügen eines Risikokorrelations-Managers 138
- Historische Korrelation 138
- Korrelationsmodul 136
- Korrelationsmodule 136
- Risikokorrelations-Bewertung, Hinzufügen 138
- Risikokorrelationsmodul 136
- Zusammenfassung 12, 62

Active Directory
- Abrufen von Daten 322
- Anmeldung, Authentifizierung 201
- Konfigurieren von Authentifizierungseinstellungen 204

Adiscon, Datenquelle, Setup 113
ADM
- Einstellungen 140
- Ereignisse 140
- Zusammenfassung 12, 62

ADM-Regeln
- Begriffstypen 149
- Dateiübertragungsprotokoll, Module 153
- DNA-Protokollanomalien für ADM-Regeln 154
- E-Mail-Protokoll, Module 153
- Hinzufügen, neu 353
- IP-Protokollanomalien für ADM-Regeln 154
- Literale 146
- Logische Elemente 354
- Logische Elemente, Bearbeiten 355
- Messgrößenreferenzen 151
- Operatoren 146
- Protokollanomalien 154
- Protokollspezifische Eigenschaften 153
- Reguläre Ausdrücke, Grammatik 146
- Syntax 146
- TCP-Protokollanomalien für ADM-Regeln 154
- Unterstützte Anwendungen und Protokolle 344
- Verwalten, benutzerdefiniert 358
- Web-Mail-Protokoll, Module 153

ADM-Regeln *(Fortsetzung)*
- Wichtige Konzepte 344

ADM-Sitzungsanzeige, Anzeigen von Kennwörtern 142
ADM-Wörterbücher 142
- Beispiele 144
- Einrichten 142
- Verwalten 145
- Verweisen auf 146

Aggregation
- Ändern der Einstellungen in Ansicht 287
- Ändern der Regeleinstellungen 373
- Beschreibung 49, 256
- Einstellungen für Gerät 50, 257
- Hinzufügen von Ausnahmen 50, 258
- Verwalten von Ereignisausnahmen 50, 258

Akkumulator-Indizes, Erhöhen der Anzahl der verfügbaren 196
Akkumulator-Indizierung, Verwalten 198
Aktionen
- Datenquellen 103
- Definieren für DEM 157
- Hinzufügen zu DEM 158
- Symbolleiste 29, 33
- Zuordnungen 103

Aktivieren des FIPS-Modus 21
Aktualisieren der DEM-Lizenz 156
Aktualisieren der ESM-Software 23
Aktualisieren der Gerätesoftware 39, 45
Aktualisieren von Geräten 60
Aktualisierter Regelstatus, Löschen 369
Aktualisierung
- Software auf mehreren Geräten 56
- Status für Geräte, Anzeigen, Richtlinien 362

Aktualisierungen
- Abrufen von Regeln 369
- Überprüfen für Regel 24

Alarm
- Verwalten von Abfragen 215, 216

Alarme
- Aktivieren 247
- Anpassen der Übersicht 248
- Anzeigen von Details 249
- Audiodateien, Verwalten 249
- Beauftragter, Ändern 249, 275
- Benachrichtigung bei Stromausfällen 190, 238

Alarme *(Fortsetzung)*
Benachrichtigungen 178
Benachrichtigungen, Hinzufügen von Empfängern 179
Bereich 29
Bereich, Anzeigen 30, 200
Berichte, Anzeigen und Verwalten 250
Berichtsdateien, Verwalten 251
Bestätigen 249
Deaktivieren 247
Einrichten und Verwalten 231
Erstellen 232
Erstellen, neu aus Ereignisansicht 287
Hinzufügen eines Integritätsüberwachungsereignisses 239
Hinzufügen zu Regel 237
Kopieren 247
Löschen 249
Protokoll 231
Schweregradsymbole 231
Threat Intelligence Exchange-Alarme 167
Verwalten von Empfängern 249
Vorlagen, Hinzufügen 248
Vorlagen, Verwalten 248
Alarmvorlagen
Bearbeiten 248
Hinzufügen 248
Kopieren 248
Standard, Festlegen 248
Alte Ressourcen, Definieren 318
Altiris-Server, Abrufen von Daten 322
Analysebericht, Generieren, IPS 172
Andern von Regeln 363
Änderungsverlauf, Anzeigen für Regeln 370
Anhalten mehrerer Geräte 56
Anhalten von Geräten 47
Anmeldeinformationen für die ePO-Authentifizierung 165
Anmeldeinformationen für ePO 165
Anmeldeinformationen, Anfordern und Hinzufügen von Regelaktualisierungen 23
Anmeldeseite, Anpassen 22
Anmeldung
Definieren von Einstellungen 201
Sicherheit 201
Zugriffssteuerungsliste (ACL, Access Control List) 202
Ansichten
Abfragen von ePO-Geräten 169
Ändern der Standardansicht 295
Bereich 29
Daten in einer Ansicht 296
Datendetails 283
Erweiterte ELM-Suche 274
Filter 296
Filtern 296
Fluss 273
Hinzufügen, benutzerdefiniert 277
Hostnamen, Anzeigen anstelle der IP-Adresse 277
Ansichten *(Fortsetzung)*
Komponenten 278
Komponenten-Symbolleiste 283
Komponenten, Anpassen 280
Komponenten, Beschreibung 279
Symbolleiste 29, 271
Verwalten 294
Vordefiniert 272
Ansichtsbereich, Einstellungen 30
Anwenden von Konfigurationseinstellungen auf DEM 157
Anzeigen
Verwalten von Abfragen 215, 216
Anzeigetyp, Auswählen 26, 54
Archiv
Einrichten inaktiver Partitionen 197
Einstellungen, Definieren für Empfänger 73
ArcSight, Hinzufügen einer Datenquelle 111
ASN
Definieren von Einstellungen für Gerät 48, 256
Suche, Ausführen 289
Suchen aus Ansicht 287
ASP-Regeln
Festlegen der Reihenfolge 341
Zeitformate, Hinzufügen 341
Asset-Manager 325
Audiodateien, Verwalten von Alarmen 249
Aufgliedern der Ansicht 287
Ausführungsverlauf für TIE 287
Ausgelöste Alarme
Anzeigen von Details 275
Bearbeiten 275
Bestätigen 275
Erstellen eines Falls 275
Filtern 275
Löschen 275
Ausnahmen für Aggregationseinstellungen, Hinzufügen 50, 258
Ausnahmen, Hinzufügen, Firewall-Regel 338
Auswahlregel für virtuelle Geräte, Verwalten 53
Authentifizierung für ePO 165
Automatisch erlernte Datenquellenregeln, Verwalten 343
Automatische Aufnahme in die Blacklist, Konfigurieren 174
Automatische Aufnahme in die Blacklist, Regeln 366
Automatisches Erstellen von Datenquellen 79
Automatisches Erstellen von Datenquellen, Regeln, Hinzufügen 80
Automatisches Lernen von Datenquellen, Einrichten 99

B

Bearbeiten eines ausgelösten Alarms 275
Bedingung, Hinzufügen, Bericht 265
Bedrohungen
Aktivieren oder Deaktivieren für Risikoberechnung 326
Anzeigen von Details 326
Bedrohungsverwaltung 325
Begriffstypen für ADM-Regeln 149

Beibehaltung, Einrichten von Datenlimits 197
Benachrichtigung, Konfigurieren, SNMP 43
Benutzer
  Arbeiten mit 199
  Authentifizieren gegenüber LDAP-Server 205
  Deaktivieren 205
  Erneutes Aktivieren 205
  Hinzufügen 200
  Hinzufügen der CAC-Anmeldung 203
  Standardname 21
Benutzerdefiniert
  Typfilter 303
Benutzerdefinierte Anzeige, Hinzufügen, Bearbeiten, Löschen 26, 54
Benutzerdefinierte ASP-Regeln, Hinzufügen 341
Benutzerdefinierte Datenquellentypen 99
Benutzerdefinierte Regeln
  Anzeigen 363
Benutzerdefinierte Typen
  Erstellen 305
  Hinzufügen, Uhrzeit 309
  Name/Wert 309
  Vordefiniert 305
Benutzerdefinierte Typen, Uhrzeit, Hinzufügen 309
Benutzerdefinierter Typ
  Hinzufügen einer Name/Wert-Gruppe 309
Benutzeridentifizierung
  Hinzufügen einer Regel 161
  Verwalten 160
Bericht
  Verwalten von Abfragen 215, 216
Berichte
  Abfragen von ePO-Geräten 169
  Alarmwarteschlange 250
  Benachrichtigungen, Hinzufügen von Empfängern 179
  Benutzerdefiniert 263
  Direkt nach der Installation verfügbar 263
  Einschließen eines Bilds 265
  Ereigniszeitpunkt 177
  ESM, Anzahl der Gerätetypen 177
  Fallverwaltung, Generieren 315
  Gerätezusammenfassung 56
  Hinzufügen 264
  Hinzufügen einer Bedingung 265
  Host-Namen anzeigen 266
  IPS-Analyse, Generieren 172
  Layout 265
  Quartalsweise, Festlegen des Startmonats 264
Bestätigen eines ausgelösten Alarms 275
Bewertung, Risikokorrelation 138
Bilder
  Einschließen in PDF-Dateien und Berichte 265
  Hinzufügen zu Anmeldeseite 22
Binden von Komponenten 292
Blacklist
  Aus Ereignis in Ansicht 287
  Einrichten, global 219
  Eintrag, Hinzufügen oder Löschen, entfernt, McAfee Network Security Manager 176
  Global 218
  Hinzufügen eines McAfee Network Security Manager-Eintrags 176
  IPS oder virtuelles Gerät 173
  Konfigurieren der automatischen Aufnahme in die Blacklist 174
  Regeln, automatisch 366
  Verwalten, IPS 174
Build, Anzeigen, Software 47

C

CAC
  Anmeldung, Einrichten 203
  Authentifizierung 201
  Einstellungen 203
  Hinzufügen von Benutzern 203
Check Point-Datenquellen, Einrichten 117
Client-Datenquellen 82
  Hinzufügen 83
  Suchen 83
Codierung für ASP-Datenquelle 109
Common Criteria-Konfiguration 20
Common Event Format, Datenquellen 112
Computer-ID, Anzeigen, Gerät 47
contains-Filter 266
CSV-Abfrageberichte 178

D

DAS, Zuweisen zum Speichern von ELM-Daten 129
Dateierweiterungen für Exportdateien 16
Dateifreigabe, Deaktivieren, Heimnetzgruppe 124
Dateiübertragungsprotokoll, Module für ADM-Regeln 153
Dateiwartung, Verwalten 209
Datenanreicherung 220
  Abfragen von ePO-Geräten 169
  Hinzufügen von Quellen 220
Datenbank
  Audit-Listen 359
  Audit-Listen, Einrichten, Regel und Bericht 359
  Server, Hinzufügen 162
  Speicherverwendung 199
  Status 177
  Verwalten 195
  Verwalten von Indexeinstellungen 198
Datenbankregeln
  Hinzufügen, neu 353
  Logische Elemente 354
  Logische Elemente, Bearbeiten 355
Datenbeibehaltungs-Limits, Einrichten 197

Datenerfassung
Aktivieren, McAfee Risk Advisor 166
McAfee Risk Advisor 166
Datenquelle
Nicht mit ESM synchronisiert 80
Datenquellen 74
Adiscon-Setup 113
Anzeigen der generierten Dateien 99
Anzeigen, Deaktiviert 30, 200
ASP-Codierung 109
Automatisches Erstellen 79
Automatisches Lernen, Einrichten 99
Benutzerdefinierte Typen 99
Check Point, Einrichten 117
Client 82
Client, Hinzufügen 83
Client, Suchen 83
Codierung für ASP 109
Common Event Format 112
Erweiterter Syslog-Parser 104
Hinzufügen 74
Hinzufügen von ArcSight 111
Hinzufügen, untergeordnet 82
IBM ISS SiteProtector 116
Importieren einer Liste 83
Importieren, Tabelle 85
Konfigurieren von ePolicy Orchestrator 4.0 111
Korrelation 102
McAfee ePO 115
Migrieren zu einem anderen Empfänger 97
Regeln für automatisches Erstellen, Hinzufügen 80
Schweregrade und Aktionen, Zuordnungen 103
Security Device Event Exchange (SDEE) 110
Tabelle zum Importieren 85
Uhrzeit nicht mit ESM synchronisiert 81
Unterstützt 100
Unterstützung für Syslog-Relay 114
Verschieben auf ein anderes System 97
Verwalten 75
Windows-Sicherheitsprotokolle 102
WMI-Ereignisprotokoll 101
Datenquellen, Regelaktionen 342
Datenquellenregeln 342
Automatisch erlernt, Verwalten 343
Datenspeicher
Einrichten der ESM-VM 196
Einrichten von ESM 196
Datenspeicher, Hinzufügen, ELM, gespiegelt 126
Datenspeicher, Spiegeln, ELM 126
Datenspeicher, Vorbereiten zum Speichern von ELM-Daten 121
Datenverkehr mit Priorität, Manager 375
Datenzugriffsregeln, Hinzufügen oder Bearbeiten 358
Datenzuordnung, Definieren von Limits 198
Datumsformat, Ändern 30, 200
Deaktivieren der SSH-Kommunikation mit ESM 48
Deaktivieren eines ELM-Spiegelgeräts 127
Deep Packet Inspection-Regeln 338
Attribute, Hinzufügen 339
Hinzufügen 338
DEM
Aktualisieren der Lizenz 156
Bearbeiten einer benutzerdefinierten Aktion 159
Benutzeridentifizierung 160
Datenbank-Server, Hinzufügen 162
Definieren von Aktionen 157
Erweiterte Einstellungen, Konfigurieren 157
Festlegen des Vorgangs 159
Hinzufügen einer Aktion 158
Konfigurationseinstellungen, Anwenden 157
Masken für vertrauliche Daten 159
Regel, Messgrößenreferenzen 348
Regeln 345
Synchronisieren von Konfigurationsdateien 157
Zusammenfassung 12, 62
DEM-Regeln
Verwalten, benutzerdefiniert 358
DEM-spezifische Einstellungen 155
DESM, Zusammenfassung 12, 62
DHCP, Einrichten 185
Direkt nach der Installation verfügbare Ansichten 272
DNA-Protokollanomalien für ADM-Regeln 154
Dokumentation
Produktspezifisch, suchen 10
Typografische Konventionen und Symbole 9
Zielgruppe dieses Handbuchs 9
Doppelte Geräteknoten, Löschen 28, 55
Durchsuchen der Referenz aus Ansicht 287
Durchsuchen von ELM 287

E

E-Mail
Einstellungen 178
Fallbenachrichtigung 314
E-Mail-Protokoll, Module für ADM-Regeln 153
E-Mail-Server, Verbinden 178
Einstellungen, Konsole 29
ELM
Abrufen von Daten 135
DAS-Gerät zum Speichern von ELM-Daten 129
Deaktivieren eines Spiegelgeräts 127
Definieren eines alternativen Speicherorts 135
Einrichten der Kommunikation mit 44
Externer Datenspeicher 128
Formatieren eines SAN-Speichergeräts zum Speichern von Daten 129
Gespiegelte Verwaltungsdatenbank, Ersetzen 135
Gespiegelter Datenspeicher, Hinzufügen 126
Gespiegelter Speicherpool, erneutes Erstellen 127
Hinzufügen eines gespiegelten Datenspeichers 126
Hinzufügen eines iSCSI-Geräts als Speicher 128

ELM *(Fortsetzung)*
Hinzufügen eines Speichergeräts 124
Integritätsprüfung, Anzeigen der Ergebnisse 132
Integritätsprüfungsauftrag 135
Integritätsprüfungsauftrag, Erstellen 136
Komprimierung 132
Komprimierung, Festlegen 132
Migrieren der Datenbank 134
Protokolldaten, Wiederherstellen 133
Schnellere Suchvorgänge, Ermöglichen 134
Sichern 133
Speichern von Protokollen 123
Speicherpool, Hinzufügen oder Bearbeiten 125
Speicherverwendung, Anzeigen 134
Speicherzuordnung, Verringern 125
Spiegeln des Datenspeichers 126
Suchansicht 274
Suchauftrag 135
Suchauftrag, Anzeigen der Ergebnisse 132
Suchauftrag, Erstellen 136
Suche, Erweitert 275
Synchronisieren mit Gerät 44
Verschieben eines Speicherpools 125
Verwaltungsdatenbank, Wiederherstellen 133
Vorbereiten zum Speicherung von Daten 121
Wiederherstellen 133
Zusammenfassung 12, 62
ELM-Einstellungen 120
ELM-Redundanz
Anhalten der Kommunikation mit dem ELM-Standby-Gerät
Anzeigen von Details der Datensynchronisierung 130
Deaktivieren der Redundanz 130
Wechseln von ELM-Geräten 130
Wiederinbetriebnehmen des ELM-Standby-Geräts 130
ELM-Speicher, Schätzen des Bedarfs 120
Empfänger
Archiveinstellungen, Definieren 73
Archivieren von Rohdaten 72
Datenquellen 74
Hinzufügen 179
Konfigurieren von Einstellungen 63
Ressourcenquelle, Hinzufügen 119
Ressourcenquellen 119
Streaming-Ereignisse, Anzeigen 63
Verwalten von Alarmen 249
Empfänger mit Fehlern, Ersetzen 72
Empfänger mit Hochverfügbarkeit 63
Empfänger-HA 63
Einrichten von Geräten 67
Erneutes Initialisieren des sekundären Geräts 68
Ersetzen eines Empfängers mit Fehlern 72
Fehlerbehebung, Fehler 72
Netzwerk-Ports 66
Überprüfen des Status 70
Upgrade 70
Empfänger-HA 63 *(Fortsetzung)*
Wechsel von Rollen 69
Endgeräte-Einstellung für Netzwerkerkennung 321
Endpunkterkennung 320
Entdecken des Netzwerks 319
Entdecken von Endpunkten 320
Entdeckung von Anomalien
Assistent 171
Variablen, Bearbeiten 172
Entdeckung von Port-Scans 335
Entfernter Blacklist-Eintrag, McAfee Network Security Manager, Hinzufügen oder Löschen 176
ePO
Hinzufügen von Anmeldeinformationen für die Authentifizierung 165
Streaming-Ereignisse, Anzeigen 63
ePO-Geräte
Abfrage für Berichte oder Ansichten 169
Abfrage für Real Time for McAfee ePO-Dashboard 170
Abfragen nach einer Datenanreicherung 169
ePolicy Orchestrator
Einstellungen 164
Konfigurieren von Version 4.0 111
McAfee Risk Advisor-Datenerfassung, Aktivieren 166
Starten über ESM 164
Tags, Zuweisen zu IP-Adresse 166
Ereignisse
Abrufen 255, 256
Beschreibung 253
Blacklist aus 287
Einrichten von Downloads 48, 254
Erstellen eines Falls zum Verfolgen 312
Festlegen des Schwellenwerts für Inaktivität 255
Hinzufügen zu einem Fall 312
Löschen 287
Markieren als überprüft 287
Protokoll, Verwalten von Ereignistypen 212
Protokolle, Festlegen der Sprache 25, 214
Schweregrad, Gewichtungen, Einrichten 374
Sitzungsdetails, Anzeigen 271
Überprüfen auf 255
Untersuchen umliegender Ereignisse auf übereinstimmende Felder 294
Verwalten von Aggregationsausnahmen 50, 258
Ereignisse und Flüsse abrufen, Symbol 33
Ereignisse, Flüsse und Protokolle
Begrenzen der Erfassungszeit 254
Ereignisweiterleitung
Agenten 260
Aktivieren oder Deaktivieren 261
Ändern von Einstellungen 261
Bearbeiten von Filtereinstellungen 262
Einrichten 259
Hinzufügen von Filtern 262
Hinzufügen von Zielen 259
Konfigurieren 259

Ereigniszeitpunkt, Bericht 177
Erfassung
SIEM Collector 75
Erneutes Erstellen eines gespiegelten Speicherpools 127
Erneutes Initialisieren des sekundären Empfänger-HA-Geräts 68
Ersetzen eines Empfänger-HA mit Fehlern 72
Erweiterte DEM-Einstellungen, Konfigurieren 157
Erweiterter Syslog-Parser
Datenquellen 104
Hinzufügen einer benutzerdefinierten Regel 341
Regeln 340
Erweiterter Syslog-Parser, Datenquelle
Codierung, andere als UTF-8 109
ESM
Aktualisieren der Software 23
Anzeigen von Systeminformationen 177
Datenspeicher, Einrichten 196
Ersetzen eines redundanten ESM-Geräts 210
IPMI-Port, Einrichten 183
Nicht mit Datenquelle synchronisiert 80
Protokollierung, Einrichten 214
Redundant, Funktionsweise 209
Redundantes ESM-Gerät 207
Regeln 360
Sicherheitsfunktionen 201
Sichern der Einstellungen 207
Sicherungsdateien 208
Steuern des Netzwerkverkehrs 184
Synchronisieren mit Gerät 43
Uhrzeit nicht mit Datenquelle synchronisiert 81
Upgrade, primär und redundant 216
Verwalten 211
Wiederherstellen der Einstellungen 207
Zusammenfassung 12, 62
Event Receiver
Zusammenfassung 12, 62
Exportieren
Anzeigen 287
Kommunikationsschlüssel 214
Komponente 289
Regeln 365
Schlüssel 38
Exportieren und Importieren
EXK-Datei 17
PUK-Datei 17
Exportieren von Zonen 323
Externe API
Verwalten von Abfragen 215, 216
Externer ELM-Datenspeicher 128

F

Fälle
Anpassen der Übersicht 248
Anzeigen von Details 313
Anzeigen, alle 314
Fälle *(Fortsetzung)*
Bearbeiten 312
Berichte, Generieren 315
E-Mail-Benachrichtigung 314
E-Mail, ausgewählter Fall 314
Erstellen aus Alarm 249
Erstellen aus ausgelöstem Alarm 275
Filtern 314
Hinzufügen 311
Hinzufügen von Ereignissen zu einem vorhandenen Fall 312
Quellereignisse, Anzeigen 314
Schließen 312
Senden einer E-Mail beim Hinzufügen oder Ändern 314
Status, Hinzufügen 313
Status, Hinzufügen oder Bearbeiten 314
Fälle, Bereich 29
Fallverwaltung
Bereich, Anzeigen 30, 200
Berichte, Generieren 315
Farbdesign, Konsole 30
Fehlerbehebung
Empfänger-HA-Fehler 72
Fehlerbehebung, FIPS-Modus 20
Filter
Ansichten 296
Ausgelöster Alarm 275
Benutzerdefinierter Typ 303
Bereich 29
Für Benutzer sichtbar und alle, Wechseln 297
Hinzufügen von Regeln 340
Hinzufügen zu verteiltem ESM-Gerät 163
Optionen, Hinzufügen und Entfernen 297
Speichern aktueller Werte als Standard 297
Standard verwenden 297
Symbolleiste 297
UCF 299
Vorhandene Regeln 367
Windows-Ereignis-ID 299
Filter, contains 266
Filter, Ereignisweiterleitung 262
Filtereinstellungen, Bearbeiten, Ereignisweiterleitung 262
Filterregeln
Datenreihenfolge 340
Festlegen der Reihenfolge 341
Regelreihenfolge 340
Filtersätze
Verwalten 297
FIPS-Modus
Aktivieren 14
Auswählen 14
Dateierweiterungen 16
Entfernte Funktionen 14
Fehlerbehebung 20
Funktionen, die nur im FIPS-Modus verfügbar sind 14
Gerät mit festgelegtem Schlüssel, Hinzufügen 16

FIPS-Modus *(Fortsetzung)*
Kommunizieren mit mehreren ESM-Geräten 17
Nicht konforme verfügbare Funktionen 14
Sichern von Informationen 16
Terminologie 16
Überprüfen der Integrität 15
Wiederherstellen von Informationen 16
Firewall-Regeln 336
Erstellen aus Ereignis oder Fluss 287
Hinzufügen von Ausnahmen 338
Hinzufügen, benutzerdefiniert 337
Typen 336
Zugreifen 172
Flüsse
Abrufen 255, 256
Ansichten 273
Beschreibung 253
Einrichten von Downloads 48, 254
Festlegen des Schwellenwerts für Inaktivität 255
Löschen 287
Überprüfen auf 255
Flussprotokollierung, Aktivieren 273

G

Geolocation, Definieren von Einstellungen für Gerät 48, 256
Gerät, Anzeigetyp, Auswählen 26, 54
Geräte
Aggregationseinstellungen 50, 257
Aktualisieren 60
Aktualisieren der Software 39, 45
Ändern der Beschreibung 47
Ändern der Standardanzeige 30, 200
Ändern des Namens 47
Anhalten 47
Anordnen 26, 39, 54
Anzahl, Bericht 177
Anzeigen allgemeiner Informationen 47
Anzeigen von Protokollen 57
Anzeigetyp 33
Anzeigetyp, Feld 33
ASN, Definieren von Einstellungen 48, 256
Build 47
Computer-ID 47
Deaktivieren von Datenquellen 30, 200
Einrichten von Downloads für Ereignisse, Flüsse und Protokolle 48, 254
Exportieren eines Schlüssels 38
Geolocation, Definieren von Einstellungen 48, 256
Gerätestatistik 45
Gewähren des Zugriffs 46
Gruppenknoten, Löschen 28, 60
Hinzufügen eines URL-Links 47, 56
Hinzufügen zur Konsole 25, 36
Importieren eines Schlüssels 38
IPMI-Port, Einrichten 183
Geräte *(Fortsetzung)*
Linux-Befehle 46
Löschen 33
Löschen von Knoten 28, 60
model 47
Nachrichtenprotokoll 45
Neu starten 47
NTP-Server 43, 179
Schlüssel 37
Seriennummer 47
Software, Aktualisieren 39, 45
Starten 47
Statusdaten, Herunterladen 45
Steuern des Netzwerkverkehrs 40
Synchronisieren der Uhren 187
Synchronisieren mit ESM 43
Überwachen des Datenverkehrs 46
Verbindung mit ESM, Ändern 48
Version 47
Verwalten mehrerer 56
Verwalten von Schlüsseln 37
Verwalten von SSH-Kommunikationsschlüsseln 38
Zusammenfassungsberichte 56
Gerätegruppe, Verwalten 27, 55
Geräteknoten, Löschen von Duplikaten 28, 55
Gerätesymbol, Hinzufügen 33
Gespiegelte Verwaltungsdatenbank, Ersetzen, ELM 135
Gespiegelter Datenspeicher, Hinzufügen, ELM 126
Gespiegelter Speicherpool, erneutes Erstellen 127
Gewichtungen, Einrichten, Schweregrad 374
Gleichzeitige Geräte für Netzwerkerkennung 321
Global Threat Intelligence-Überwachungsliste 300
Globale Blacklist 218
Einrichten 219
Gruppen
Benutzer 199
Einrichten von Benutzern 206
GTI-Überwachungsliste 300

H

Hadoop Pig 222
Handbuch, Informationen 9
Hardware 177
Heimnetzgruppe, Dateifreigabe, Deaktivieren 124
Heruntergeladene Regeln, Überschreibungsaktion 373
Herunterladen
Ereignisse, Flüsse und Protokolle 48, 254
Hierarchische ESM-Geräte, Maskieren von Daten 213
Hinzufügen einer Teilzone 324
Historische Korrelation, ACE 138
Historische Korrelation, Ereignisse herunterladen 139
Historische Korrelation, Hinzufügen eines Filters 139
Host-Namen, Anzeigen in Bericht 266
Hostnamen
Verwalten 185

I

IBM ISS SiteProtector-Datenquelle 116
Importieren
  Datenquellenliste 83
  Geräteschlüssel 38
  Regeln 364
  Variable 333
  Zeichenfolgennormalisierungs-Datei 302
Importieren von Datenquellen, Tabelle 85
Importieren von Zoneneinstellungen 323
In ESM verfügbare VA-Anbieter 78
Inaktive Partitionen, Archiv, Einrichten 197
Indexeinstellungen, Datenbank 198
Indizes, Erhöhen der verfügbaren, Akkumulator 196
Indizierung, Akkumulator 198
Information, Kennzeichnungen 57
Integritätsprüfung, Anzeigen der Ergebnisse 132
Integritätsprüfungsauftrag 135
  Erstellen 136
Integritätsstatus, Kennzeichnungen 33, 57
Integritätsüberwachung
  Signatur-IDs 239
Interne Regeln 339
  Verwalten 339
Internetquellen
  Erstellen einer Watchlist 300
IP
  Adresse, Zuweisen von ePolicy Orchestrator-Tags 166
IP-Ausschlussliste, Verwalten 320
IP-Protokollanomalien für ADM-Regeln 154
IPMI-Port, Einrichten in ESM oder auf Geräten 183
IPMI-Port, Konfigurieren des Netzwerks 183
IPS
  Analysebericht, Generieren 172
  Assistent zur Entdeckung von Anomalien 171
  Automatische Aufnahme in die Blacklist, Konfigurieren 174
  Blacklist 173
  Blacklist, Verwalten 174
  Datenverkehr mit Priorität, Variable 375
  Entdeckung von Anomalien, Variablen, Bearbeiten 172
  Interne Regeln 339
  Konfigurieren von Einstellungen 170
  Reiner Warnungsmodus 361
iSCSI-Gerät, Hinzufügen als ELM-Speicher 128

K

Kategorie
  Bearbeiten 372
  Hinzufügen einer neuen Variablen 333
  Hinzufügen neuer Tags 372
Kennwörter
  Ändern 30, 200
  Standard 21
Kennwörter in der Sitzungsanzeige, Anzeigen 142
Kennzeichnung, ePO 165
Kennzeichnungen, Gerät oder System 57
Kommunikationsschlüssel, Exportieren und Wiederherstellen 214
Komponenten
  Anpassen 280
  Ansichten 279
  Anzeigen 278
  Beispiel für Regel 356
  Binden 292
  Exportieren 289
  Hinzufügen von Parametern 355
  Menüoptionen 287
  Symbolleiste 283
Komprimierung, Festlegen, ELM 132
Komprimierung, Verwalten, ELM 132
Konfigurationsdateien, Synchronisieren von DEM 157
Konfigurationseinstellungen, Anwenden auf DEM 157
Konfigurationsverwaltung 318
Konsole
  Ändern der Darstellung 30, 200
  Diagramm 29
  Farbdesign 30
  Hinzufügen eines Geräts 25, 36
  Zeitüberschreitung 30
Konsoleneinstellungen 29
Konventionen und Symbole in diesem Handbuch 9
Kopieren und Einfügen von Regeln 363
Korrelationsalarm
  Einschließen von Quellereignissen 235
Korrelationsdatenquellen 102
Korrelationsereignis, Anzeigen der Quellereignisse 73
Korrelationsmodul, ACE 136
Korrelationsregeln 352
  Anzeigen von Details
    Festlegen zum Anzeigen von Details 353
  Beispiel 356
  Hinzufügen von Parametern 355
  Hinzufügen, neu 353
  Konflikte beim Importieren 364
  Logische Elemente 354
  Logische Elemente, Bearbeiten 355
  Threat Intelligence Exchange-Regeln 167
  Verwalten, benutzerdefiniert 358
Kunden-ID 177

L

Layout, Hinzufügen eines Berichts 265
LDAP
  Anmeldung, Authentifizierung 201
  Server, Authentifizieren von Benutzern 205
Limits, Einrichten für Datenbeibehaltung 197
Linux
  Befehle 217
  Verfügbare Befehle 218

Linux-Befehle, Eingeben für Gerät 46
Literale für ADM-Regeln 146
Lizenz, Aktualisieren von DEM 156
Logische Elemente für ADM-Regeln, Datenbankregeln, Korrelationsregeln 354
Logische Elemente, Bearbeiten 355
Logo, Hinzufügen zu Anmeldeseite 22
Löschen
    Ausgelöster Alarm 275
    Benutzerdefinierte Regeln 363
    Ereignisse oder Flüsse 287

M

Masken für vertrauliche Daten 159
    Verwalten 160
Maskieren von IP-Adressen 213
McAfee ePO
    Anmeldeinformationen, Einrichten für Benutzer 31, 204
McAfee ePO-Datenquellen 115
McAfee Network Security Manager
    Blacklist-Eintrag, Hinzufügen 176
    Einstellungen 176
    Entfernter Blacklist-Eintrag 176
    Hinzufügen oder Löschen 176
McAfee Risk Advisor
    Datenerfassung 166
    Datenerfassung, Aktivieren 166
McAfee ServicePortal, Zugriff 10
McAfee Vulnerability Manager
    Ausführen von Scans 175
    Einstellungen 174
    Scan, Ausführen aus Ansicht 287
    Verbindungen, Einrichten 175
    Zertifikat und Passphrase, Abrufen 175
McAfee-MIB 191
McAfee-Regelsätze 119
Mehrere Geräte
    Verwalten 56
    Verwaltungssymbol 33
Messgrößenreferenzen
    ADM-Regeln 151
    DEM-Regeln 348
Metadatenereignisse 140
MIB, McAfee 191
Migrieren der Datenbank, ELM 134
Migrieren von Datenquellen zu einem anderen Empfänger 97
Modell, Anzeigen, Gerät 47

N

Nachrichteneinstellungen 178
Nachrichtenprotokoll, Anzeigen für Gerät 45
Name/Wert-Gruppe, benutzerdefinierter Typ, Hinzufügen 309
Name/Wert, benutzerdefinierte Typen 309
Netzwerk
    Konfigurieren von Einstellungen 180
    Ports für Empfänger-HA 66
    Schnittstellen, Festlegen für Geräte 40, 181
    Topologie-Komponente, Hinzufügen von Geräten 282
    Topologie, Gerätedetails 282
    Verwalten von Schnittstellen 41, 181
Netzwerkeinstellungen
    IPMI Port, Einrichten 183
Netzwerkerkennung 319
    Konfigurationsverwaltung 318
NetzwerkerkennungEndgeräte
    Ping-Abfrageintervall 321
    Ping-Zeitüberschreitung 321
    Subnetze zum Senden des Ping-Befehls 321
Netzwerkübersicht 321
Neustarten mehrerer Geräte 56
Neustarten von Geräten 47
Nitro IPS
    Zusammenfassung 12, 62
Normalisierung 360
Normalisierung von Web-Anfragen 335
NSM
    NSM-SIEM-Konfigurations-Tool 115
    Streaming-Ereignisse, Anzeigen 63
NTP-Server
    Anzeigen des Status 180
    Einrichten für Gerät 43, 179

O

Operatoren für ADM-Regeln 146

P

Parameter, Hinzufügen zu Korrelationsregel oder -komponente 355
Partitionen, Einrichten, Inaktiv, Archiv 197
Passphrase und Zertifikat, Abrufen, McAfee Vulnerability Manager 175
PDF-Dateien, Einschließen eines Bilds 265
Ping-Einstellungen für Netzwerkerkennung 321
Ports
    Empfänger-HA, Netzwerk 66
Präprozessorregeln 335, 336
Primäres ESM-Gerät, Upgrade 216
Profil für Remote-Befehl, Konfigurieren 188
Profile, Konfigurieren 188
Protokoll
    Anomalieereignisse 140
Protokollanomalien, TCP 334
Protokolldaten, Wiederherstellen, ELM 133
Protokolle
    Beschreibung 253
    Einrichten von Downloads 48, 254
    Festlegen der Sprache 25, 214
    Typen, Generieren 213

Protokolle *(Fortsetzung)*
Überprüfen auf 255
Verwalten 212
Protokolle, Speichern, ELM 123
Protokollierung
Abmelden, Konsole 21
Aktivieren, Fluss 273
Anzeigen, System oder Gerät 57
Einrichten von ESM 214
Festlegen des Standardpools 44
Konsole, erstes Mal 21
Protokollspezifische Eigenschaften für ADM-Regeln 153

Q

Quartalsberichte, Festlegen des Startmonats 264
Quell IP-Adressen, Anzeigen des Host-Namens in Bericht 266
Quellen, Hinzufügen von Datenanreicherung 220
Quellereignisse
Einschließen in Korrelationsalarm 235
Quellereignisse, Anzeigen für Korrelationsereignis 73

R

RADIUS
Anmeldung, Authentifizierung 201
Authentifizierungseinstellungen 202
Real Time for McAfee ePO
Abfragen von ePO für Dashboard 170
Ausführen von Aktionen 167
Redundantes ESM-Gerät
Einrichten 207
Ersetzen 210
Funktionsweise 209
Speichern der Systemeinstellungen 209
Upgrade 216
Regeln
Abrufen von Aktualisierungen 369
Aktualisierung, Anmeldeinformationen 23
Ändern 363
Ändern der Aggregationseinstellungen 373
Anzeigen der Signatur 368
Anzeigen, benutzerdefiniert 363
Auslöseereignisse 140
Automatische Aufnahme in die Blacklist 366
Datenquelle 342
Erstellen, benutzerdefiniert aus Ereignis 287
Erweiterter Syslog-Parser 340
Exportieren 365
Filtern vorhandener 367
Firewall, Zugreifen 172
Hinzufügen eines Alarms 237
Hinzufügen zu Überwachungsliste 371
Importieren 364
Intern 339
Kopieren und Einfügen 363
Regeln *(Fortsetzung)*
Löschen des Aktualisierungsstatus 369
Löschen, benutzerdefiniert 363
Normalisierung 360
Präprozessor 335, 336
Schweregrad 374
Standard, Zugreifen 172
Transaktionsüberwachung, Hinzufügen oder Bearbeiten 358
Typen und Eigenschaften 331
Überprüfen auf Aktualisierungen 24
Überschreibungsaktion für heruntergeladene 373
Variablen 332
Vergleichen von Dateien 370
Verlauf, Anzeigen von Änderungen 370
Windows-Ereignisse 343
Regelsätze 119
Reguläre Ausdrücke, Grammatik für ADM-Regeln 146
Reiner Warnungsmodus
Aktivieren 362
Richtlinien 361
Remedy
Fall-ID, Festlegen 287
Fall-ID, Hinzufügen zu Ereignisdatensatz 289
Server-Einstellungen 178
Remote-Gerät, Zugreifen 217
Ressourcen
Definieren alter Ressourcen 318
Schweregrad 374
Verwalten 318
Ressourcenquellen 321
Empfänger 119
Hinzufügen, Empfänger 119
Verwalten 322
Richtlinie
Anwenden von Änderungen 375
Anzeigen von Regeln 329
Exportieren 329
Hinzufügen 329
Importieren 329
Kopieren 329
Löschen 329
Richtlinienstruktur 328
Richtlinienstruktur, Symbole 328
Suchen 329
Umbenennen 329
Untergeordnete Richtlinie, Hinzufügen 329
Richtlinien-Editor
Änderungsverlauf 375
Anzeigen des Richtlinienaktualisierungsstatus für Geräte 362
Überbelegungsmodus, Einrichten 362
Risiko
Bei der Berechnung zu berücksichtigende Bedrohungen 326
Risikokorrelation Manager, Hinzufügen 138
Risikokorrelations-Bewertung 138

Risikokorrelationsmodul, ACE 136
RisikoschweregradBedrohungsverwaltung
    Ansichten, benutzerdefiniert und vordefiniert 325
    Verwalten 325
Rohdaten, Archivieren 72
RPC-Normalisierung 335

S

SAN Speichergerät, Formatieren zum Speichern von ELM-Daten 129
Scans, Ausführen, McAfee Vulnerability Manager 175
Schlüssel
    Exportieren 38
    Gerät 37
    Importieren 38
    Verwalten, Gerät 37
Schnellstartsymbole 29
Schnittstelle
    Netzwerkeinstellungen 40, 181
    Verwalten des Netzwerks 41, 181
Schwachstelle
    Bewertung 322
    Schweregrad 374
    Verwalten von Quellen 322
Schwellenwert für Inaktivität, Festlegen 255
Schweregrad
    Datenquellen 103
    Gewichtungen 374
    Gewichtungen, Einrichten 374
    Zuordnungen 103
SDEE-Datenquellen 110
Sekundäres Empfänger-HA-Gerät, Erneutes Initialisieren 68
Seriennummer
    Anzeigen, Gerät 47
    System 177
ServicePortal, Quellen für Produktinformationen 10
Sicherheit, SSH-Kommunikationsschlüssel 38
Sicherheitsfunktionen 201
Sichern
    ELM 133
    ESM-Einstellungen 207
    Systemeinstellungen 206
Sichern, Wiederherstellen 208
Sicherungsdateien, Arbeiten mit 208
Signatur-IDs für Integritätsüberwachung 239
Signatur, Anzeigen von Regeln 368
Sitzungsanzeige, Anzeigen von Kennwörtern 142
Sitzungsdetails, Anzeigen 271
SNMP
    Benachrichtigung bei Stromausfällen 189
    Einstellungen 188
    Konfiguration 188
    Konfigurieren von Benachrichtigungen 43
    MIB 191
Software
    Aktualisieren auf mehreren Geräten 56
Software, Aktualisieren des Geräts 39, 45
Software, Aktualisieren, ESM 23
Speicher
    Einrichten von ESM-Daten 196
    Einrichten von ESM-VM-Daten 196
Speicher, Datenbank, Verwendung 199
Speicher, ELM, alternativer Speicherort 135
Speichergerät, Hinzufügen, ELM 124
Speichern von ELM-Daten, Vorbereiten 121
Speichern von ELM-Protokollen 123
Speicherpool, erneutes Erstellen, gespiegelt 127
Speicherpool, Hinzufügen eines Speichergeräts für die Verknüpfung 124
Speicherpool, Hinzufügen oder Bearbeiten 125
Speicherpool, Verschieben 125
Speicherverwendung, Anzeigen, ELM 134
Speicherzuordnung, Verringern, ELM 125
Spiegelgerät, Deaktivieren, ELM 127
Spiegeln des ELM-Datenspeichers 126
Sprache, Festlegen für Ereignisprotokolle 25, 214
SSH
    Erneutes Generieren des Schlüssels 215
    Kommunikation, Deaktivieren mit ESM 48
    Kommunikationsschlüssel, Verwalten für Geräte 38
Standardansicht, Ändern 295
Standardanzeigetyp, Ändern 30, 200
Standardmäßiger Protokollierungspool, Festlegen 44
Standardregeln, Zugreifen 172
Starten
    ePolicy Orchestrator 287
    ePolicy Orchestrator über ESM 164
Starten mehrerer Geräte 56
Starten von Geräten 47
Statische Routen, Hinzufügen 41, 182
Statistik, Anzeigen für Gerät 45
Status
    Empfänger-HA 70
    Geräte, Anzeigen, Richtlinienaktualisierung 362
    Inaktiv 57
Status des Geräts, Herunterladen von Daten 45
Status für Fälle, Hinzufügen 313
Steuerung des Netzwerkverkehrs
    ESM 184
    Geräte 40
Streaming-Ereignisse für Empfänger, NSM, ePO 63
Suchauftrag 135
Suchauftrag, Anzeigen der Ergebnisse 132
Suchauftrag, Erstellen 136
Suche, Erweitert, ELM 275
Suchvorgänge, Ermöglichen, schneller, ELM 134
Synchronisieren der Systemzeit 186, 187
Synchronisieren des Geräts mit ESM 43

Synchronisieren von Geräten
Uhren 187
Systemeinstellungen
Sichern 206
Speichern auf redundantem ESM-Gerät 209
Wiederherstellen 206
Systemnavigation
Leiste 29
Struktur 29
Systemnavigationsstruktur
Anordnen von Geräten 39
Diagramm 33
Systemprotokoll, Anzeigen 57
Systemuhr 177

T

Tags
Bearbeiten, vorhanden 372
Benutzerdefiniert, Löschen 372
Hinzufügen, neu 372
Kategorie, Hinzufügen, neu 372
Löschen, benutzerdefiniert 372
Schweregrad 374
Zuweisen zu Regeln oder Ressourcen 372
Zuweisen, ePolicy Orchestrator zu IP-Adresse 166
Task-Manager 215, 216
TCP
Protokollanomalien 334
Übernahme der Kontrolle über Sitzungen 334
TCP-Abbild sichern, 46
TCP-Protokollanomalien für ADM-Regeln 154
Technischer Support, Produktdokumentation finden 10
Teilzonen
Hinzufügen 324
Terminal, Verwenden von Linux-Befehlen 217
Threat Intelligence Exchange
Integration in ESM
Ausführungsverlauf 167
Transaktionsüberwachungsregel, Hinzufügen oder Bearbeiten 358
Typen von Regeln 331

U

Überbelegungsmodus, Einrichten 362
Übernehmen der Kontrolle über Sitzungen, TCP 334
Überschreibungsaktion für heruntergeladene Regeln 373
Übersicht des Netzwerks 321
Überwachen des Datenverkehrs von Geräten 46
Überwachung von TCP- und UDP-Sitzungen 335
Überwachungsliste
Anfügen von Ereignissen 287
Erstellen in Ansicht 287
Erstellen, neu 370
GTI 300
Hinzufügen 299
Überwachungsliste *(Fortsetzung)*
Hinzufügen von Regeln 371
Übersicht 299
UCF-Filter 299
Uhr, Synchronisieren, Gerät 187
Uhrzeit zwischen ESM und Datenquelle nicht synchronisiert 80, 81
Uhrzeit, Synchronisieren der Uhrzeit 186
Umgehungs-Netzwerkkarte
Einrichten 42, 183
Übersicht 42, 182
Untergeordnete Datenquellen, Hinzufügen 82
Unterstützte Datenquellen 100
Unterstützung für Syslog-Relay 114
Untersuchen umliegender Ereignisse auf übereinstimmende Felder in Ereignissen 294
Upgrade
Empfänger-HA 70
Primäres und redundantes ESM-Gerät 216
URL-Link
Hinzufügen von Geräteinformationen 47
URL-Links
Hinzufügen zu Gerät 56

V

VA-Abruf, Fehlerbehebung 78
VA-Daten, Abrufen 77
VA-Daten, Integrieren 76
VA-Quelle, Hinzufügen 77
VA-Systemprofil, Definieren 77
Variablen 332
Ändern 333
Ändern des Typs 333
Benutzerdefiniert, Hinzufügen 333
Importieren 333
Kategorie, Hinzufügen, neu 333
Löschen, benutzerdefiniert 333
priority_traffic 375
Verbindungen
Ändern, mit ESM 48
Einrichten von McAfee Vulnerability Manager 175
Verfolgen eines Ereignisses 312
Vergleichen von Regeldateien 370
Vergleichen von Werten in Verteilungsdiagrammen 293
Verknüpfen von Komponenten 292
Verlauf
Anzeigen von Änderungen für Regeln 370
Richtlinienänderung 375
Verringern der ELM-Speicherzuordnung 125
Verschieben eines Speicherpools 125
Verschieben von Datenquellen auf ein anderes System 97
Verschleierung 213
Version, Anzeigen, Software 47
Verteiltes ESM-Gerät
Eigenschaften 163

Verteiltes ESM-Gerät *(Fortsetzung)*
Hinzufügen von Filtern 163
Verteilungsdiagramm, Vergleichen von Werten 293
Verwaltungsdatenbank, Wiederherstellen, ELM 133
Verweisen auf ADM-Wörterbuch 146
Virtuelle Geräte 51
Auswahlregeln, Verwalten 53
Blacklist 173
Hinzufügen zu Gerät 53
Interne Regeln 339
Reiner Warnungsmodus 361
VLAN
Ändern 287
Hinzufügen 42, 182
VM, Einrichten des Datenspeichers 196
Vordefinierte Ansichten 272
Vorgang, Festlegen für DEM 159
Vorlagen, Hinzufügen von Alarmen 248
Vorlagen, Verwalten von Alarmen 248

W

Watchlist
Threat Intelligence Exchange-Watchlist 167
Verwalten von Abfragen 215, 216
Watchlists
Internetquellen 300
Web-Mail-Protokoll, Module für ADM-Regeln 153
Wechseln zwischen Empfänger-HA-Rollen 69
WHOIS
Suche, Ausführen 289
Suchen aus Ansicht 287
Wiederherstellen
Kommunikationsschlüssel 214
Systemeinstellungen 206
Wiederherstellen der ESM-Einstellungen 207
Wiederherstellen gesicherter Konfigurationsdateien 208
Wiederherstellen von ELM aus Sicherung 133
Windows
Ereignis-ID-Filter 299
Ereignisregeln 343
Windows-Sicherheitsprotokolle 102
WMI-Ereignisprotokoll 101
Workflow Überwachung 312

Z

Zeichenfolgennormalisierung
Erstellen einer Datei zum Importieren 302
Verwalten von Dateien 302
Zeitsynchronisierung 187
Zeitüberschreitung, Konsole 30
Zeitzone
Format, Ändern 30, 200
Zertifikat
Installieren, neu 187
Passphrase, Abrufen, McAfee Vulnerability Manager 175
Ziel IP-Adressen, Anzeigen des Host-Namens in Bericht 266
Zielbasierte IP-Defragmentierung 335
Zielbasiertes Zusammensetzen von TCP-Datenströmen 335
ZipZap 335
Zonen
Exporteinstellungen 323
Hinzufügen 323
Hinzufügen einer Teilzone 324
Importieren von Zoneneinstellungen 323
Verwalten 322
Zonenverwaltung 322
Zugreifen, Remote-Gerät 217
Zugriff, Gewähren für Geräte 46
Zugriffssteuerungsliste, Einrichten 202
Zuordnung, Definieren von Datenlimits 198